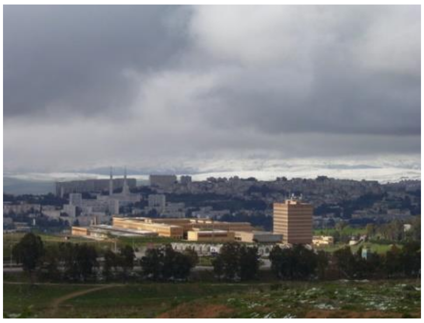
Number Theory

Ideas and Concepts

Mohammed Fulano

B.Sc. in Applied Mathematics

mohammedfulano@hotmail.com



I have uploaded this book on the web for anyone who wants to learn beginning number theory. It is for personal use only. All rights are reserved.

First Version (20/11/2018)

The book still being updated, any mistakes occurring here are mine.

Preface

Since the ancient time of the Greek Antiquity, mathematicians have been much preoccupied by the study of numbers through three branches:

a) Arithmetic[1]: study of integers $\mathbb{N}$(later also $\mathbb{Z}$) and their combinations: the rational numbers $\frac{a}{b}$ by the use the four known operations: $\pm$, $\times$, $\div$.

b) Classical algebra: called *college algebra* or sometimes simply *algebra*, the study of numbers as solutions of equations written in letters.

c) Number theory: tha part that uses complicated methods from different other disciplines to study the numbers like primes, algebraic and transcendental numbers,…

Number theory, called '*Queen of the mathematics*' , still remains today an important part of mathematics, has participated much in the creation of many branches of modern mathematics, in particular it permeated the solution of some of the great mathematical problems inherited from Greek Antiquity

− Construction of regular polygons.
− Trisection of the angle.
− Squaring the circle.
− Duplication of the cube

But despite of its attraction and its easy language understood by non-specialists, its problems are often extremely difficult to solve, we can cite for example:

i) **Goldbach** problem: every even integer $n \geq 4$ is the sum of two prime numbers

---

[1] The word *arithmetic* is very linked to the theory of numbers; we know that **Gauss** named number theory: the *Higher Arithmetic*. It is still, especially in French language, used to mean algebraic aspects in number theory references. In his book *Cours d'Arithmétique* (1970), famous French mathematician Jeans-Pierre **Serres** treated very sophistacated methods of algebraic number theory.

$ii)$ Twin primes problem: There are infinitely many primes of the form $(p_n, p_n + 2)$

These two famous conjectures remained without solution since long, despite of great efforts by many of the best mathematicians.

The invention of printing by **Gutenberg** (1400-1468) at the down of Middle Ages has permeated the publishing of books and the divulgating of science within public. Among the most influent books in this branch of mathematics, of which some are still printed even today, we can mention:

- The *Arithmetica* of **Diophantus** (210-293), a famous book in Greek published in 1621 with a Latin translation by French mathematician **Bachet** (1581-1638). This book inspired many mathematicians like **Fermat**. The book of **Diophantus** was known to Muslims, it was commented by Ahmed Sarchasi (800-865)[2]. We may also mention at its side *the Element*s of **Euclid** which contained the early results on prime numbers (parts VII, VII and IX).

- *Algebra* of Leonard **Euler** $(1707 - 1783)$ published in Saint-Petersburg in 1770 , translated into German in 1802, and then translated also into English in 1822, and in 1840. lately it has been printed by Springer(1984).

- *Théorie des Nombres* : of French mathematician **Legendre** $(1752 - 1833)$, first published in 1798, then in 1830 with supplements, it was translated into German in 1886.

- *Disquisitiones Arithmeticae* (*arithmetic researches*) : of the German mathematician Karl **Gauss**[3]$(1777 - 1849)$ published in 1801 , **Gauss** has written it in Latin. Still in print, it was first translated in German in 1805, then into French in 1812, there is also an English American edition (1966) .**Gauss** has surely mentioned his predecessors :

> *…Diophantiu's book seems to mark an epoch in the history of mathematics more because it presents the first traces of the characteristic art and Algebra than because it enriched Higher Arithmetic with new discoveries. Far …Meanwhile there appeared an outstanding work by a man to whom Higher Arithmetic already owed much.*

---

[2] Mentioned in Ibn Nadim, p. 321.

[3] **Gauss** is generally considered to be the greatest scientist in history. From before his time and until today, there has been no comparable person who has given such great different achievements, during such remote period of time, and at such an age.

Legendre's "Essai d'une théorie des nombres". Here he collected together and systematized not only all that had been discovered up to that time but also many new results of his own. Since this book came to my attention after the greater part of my work was already in the hands of the publishers, I felt obliged, however, to add Additional Notes on a few passages and I trust that this understanding and illustrious man will not be offended.

- *Lectures on Numbers Theory:* by Gustave **Dirichlet** (1809-1859) published in 1841, the 4th edition was published by **Dedekind** in 1894 with supplements, it was translated into English in 1968 (Chelsea).

- *Theory of Numbers* : of David **Hilbert** (1877-1947) published in

- *Introduction to the Theory of Numbers* : of Godfrey **Hardy** (1877-1947) and Edward **Wright** (1906-2005), the first edition was in 1938. After the death of **Hardy**, **Wright** updated its content at many occasions. It is today in its 7^{th} edition, it has been translated into French in 2007(Dunob), and into Spanish (2001).

Number theory can be classified in three big parts

$a)$ *Elementary number theory*: it studies the integers by the use of the four finite operations (×,÷ ,− ,+) , it implies often methods called *elementary* , which are not easy at all.

$b)$ *Algebraic number theory*: as its name shows, it is the study of integers by the use of algebraic structures : groups, rings, fields, ideals,… these same structures have been emerged from the problems of the theory of numbers itself.

$c)$ *Analytic numbers theory*: this branch uses les methods of Analysis like : infinite series, derivation, integration, complex variables, trigonometric sums,… to explore the proprieties of numbers.

One of the reasons perhaps, of the difficulty of elementary methods is that there is a void between integer numbers, on the contrary the system of real numbers is continuous, which facilitate the use of powerful methods, like the passage to limit of continuous functions, definite integral, continuous infinite sums,… as an example, the prime number theorem (PNT) has been proved in 1898 by analytic methods, it took 49 years for mathematicians to discover the elementary proof. Analytic methods are more successful because we have results in number theory that have been solved only by analytic methods like **Direchlet**'s theorem on primes in sequences[4].

The problems encountered in number theory may have many aspects to an extent that it is difficult to decide to which part they belong: some are elementary and analytic, others elementary and algebraic …One must get a lot of information on these branches before launching into research. My aim in this book to expose to the reader some of the ideas and methods of these three branches, and he will discover that they are much intertwined at a point that , he must at least have a general view of them, before specializing in a particular domain.

Number theory turns around the concept of *integer number*. One of the most important integers are the prime numbers that we find much in this book, and among the aspects of their importance and involvement in number theory we can cite:

− to prove the **Fermat** Last Theorem, one have to prove it only for prime numbers p_i
− a ring with prime cardinal is a field.
− the characeterestic of a field(ring) is 0 or a prime p.
−the cardinal of finite field is always of the form p^n
−**Cauchy** and **Sylow** theorems on finite groups …

There are in number theory, problems considered only as curiosities (like the perfect and amicable numbers) while others are theoretically very important, as an example the case of **Riemann** hypotheses which implies hundreds of results not proved yet, it has also played important role in the development of function theory and complex analysis, and has an obscure link with theoretical physics. Another example in the history of mathematics which is dramatically the inverse, was **Fermat** Last Theorem, it was not at all as important as the **Riemann** hypotheses but the search for its solution has created whole branches of modern mathematics, which have turned to be more important

---

[4] This was a mistake, it appears that **Silberg** gave an elementary proof in 1949, see also **Trost** : *Primzahlen*(1966) p. 75.

than the theorem itself.
Number theory has seen big leaps during the XX century, mainly because of the ***Hilbert**ʹs 23 problems (1900)*, six of them were in number theory (problems : 7, 8,9 and 11) :

− the nature of the numbers a^b, where a est algebraic and b irrational.
− the **Riemann** hypothesis, **Goldbach** conjecture, twins conjecture.
− the reciprocity law in number fields.
− classification of quadratic forms in number fields.

We cannot give all things in one book; then it has been a question of making choices. I have tried to give the necessary to familiarize the reader with the concepts.

I have read a lot of great specialists of number theory, and also vulgarization books that you will find in the bibliography. I have tried as much as possible to give motivations and useful historical details. The history of mathematics does not teach mathematics, but can give some useful clarifications. When the student is given reasons why mathematicians are lead to this, and why they did that ,and so on… helps him to feel at ease when he is doing mathematics.

To learn mathematics one must solve lots and lots of exercises. The book is a *problem book* where I have proposed a lot of exercises not very difficult to which the reader ought to participate in order to advance step by step in this difficult domain. Above all, he must not be discouraged if he makes mistakes, even genius mathematicians have made mistakes. It is by struggling with the exercises that he will learn skills and becomes a talented number theorist.

Although this is a preparative text (I originally wrote it in French I am now progressively translating it into English), I would be very happy if it will be at the good hope of all readers who are interested in this beautiful branch of mathematics.

mohammedfulano@hotmail.com

Notation and conventions

A number x is *positive* if : $x > 0$

A number x is *nonnegative* if : $x \geq 0$

The sentence : “Let n be an integer” means : $n \in \mathbb{Z}$

The sentence : “let n be a natural integer” means : $n \in \mathbb{N}$

In what follows , $\boldsymbol{p}$ is always a prime number.

■ : After the end of a proof, in other books you can find the latin $\boldsymbol{QED}$ or the French $\boldsymbol{CQFD}$.

Contents

First part: Elementary number Theory

Chapter 1 : **Recreational number theory**

— From the Greeks to Fermat……………………………………………………………**9**
— methods of proof……………………………………………………………………
— perfect…………………………………………………………………………………
— Euclidian division……………………………………………………………………
— proprieties des divisors of an integer n…………………………………………
— primes…………………………………………………………………………………
— perfect numbers ………………………………………………………………………
—**Exercices**…………………………………………………………………………………

Chapter 2 : **The set of integer numbers $\mathbb{Z}$**

— From the Greek to Euler……………………………………
— divisibility in $\mathbb{Z}$……………………………………
— divisors……………………………………
— Euclidian division……………………………………
— proprieties des divisors of an integer n……………………………………
— primes……………………………………
— perfect numbers ……………………………………
—**Exercices**…………………………………………………………………………………

Chapter 3 : congruences
—residus modulo n…………………
—primitives roots…………………
— reciprocity law…………………
— Chinese remainder theorem…………………
—**Exercices……………………………………………………………………………………..**

Chapter 3 : Proprieties of prime numbers
— arithmétic functions
—Eratosthenes sieve
—twines conjecture
—distributions of primes
—Exercices

Chapter 4 : Diophantine equations
—congruent numbers
—Bézout_equality
— the Pell equation
—Exercices

Chapitre 5 : Partitions theory
—la
—les nombres p
— Waring problem
—Exercices

Chapter 6 : Quadratic forms
— L'égalité de Bézout
— class number
— Direchlet
—Exercices

Chapitre 5 : Bernoulli numbers
—la divisibilité dans $\mathbb{Z}$
—les nombres parfaits
—Exercices

Chapter 7 : **Transcendental numbers**

— Irrationnel numbers……………………………………………………………………………
— nombres algebraic numbers ……………………………………………………………
—**Exercices**……………………………………………………………………………………………

Open problems……………………………………………………………………

Second part: Algebraic number Theory

Chapter 1 : **origins of algebraic number theory**

—racines primitives………………………………………………………………………
—grand theorem de Fermant………………………………………………………………
—Kummeret les nombres cyclotomiques…………………………………………………………
— algebric equations………………………………………………………………

—**Exercices**……………………………………………………………………

Chapitre 1 : algebraic Structures

—groupes
—anneaux
—corps
—espaces vectoriels
—Exercices

– Chapitre 1 : theory of algebraic numbers

–
–grand
–Kummer
–les
–Exercices

Chapitre 1 : Factorial rings

–
–grand
–Kummer
–Exercices

– Chapitre 1 : Galois theory

–
–grand
–Kummer
–les
–Exercices

– Chapitre 1 : p-adiques nombres

–
–grand
–Kummer
–Exercices

Chapitre 1 : quadratic forms

–
–grand
–Kummer
–Exercices

Chapitre 1 : algebraic fields

–
–grand
–Kummer
–Exercices

Chapitre 1 :Théorie de corps de classes

—
—grand
—Kummer
—les
—Exercices

Open problems

Third part: Analytic number Theory

Chapitre **1 the infinite orders**

—
—Landau notation
— Vinogradov notation
— Vinogradov notation
—Exercices

Chapitre 1 : **Dirichlet's work**

—
—grand
—Kummer
—Exercices

Chapitre 1 : **distribution des nombres premiers**

—
—grand
— la fonction zeta
—Exercices

Chapitre 1 : **multiplicative number theory**

—
—grand
— la fonction zeta

—Exercices

Chapitre 1 : **les fonction L_χ**
—la fonction zeta
—la fonction
— tauberian thoery
—Exercices

Chapitre 1 : **les fonctions automorphes**
—la
—la
—la fonction
—Exercices

Chapitre 1 : **Additive number theory**

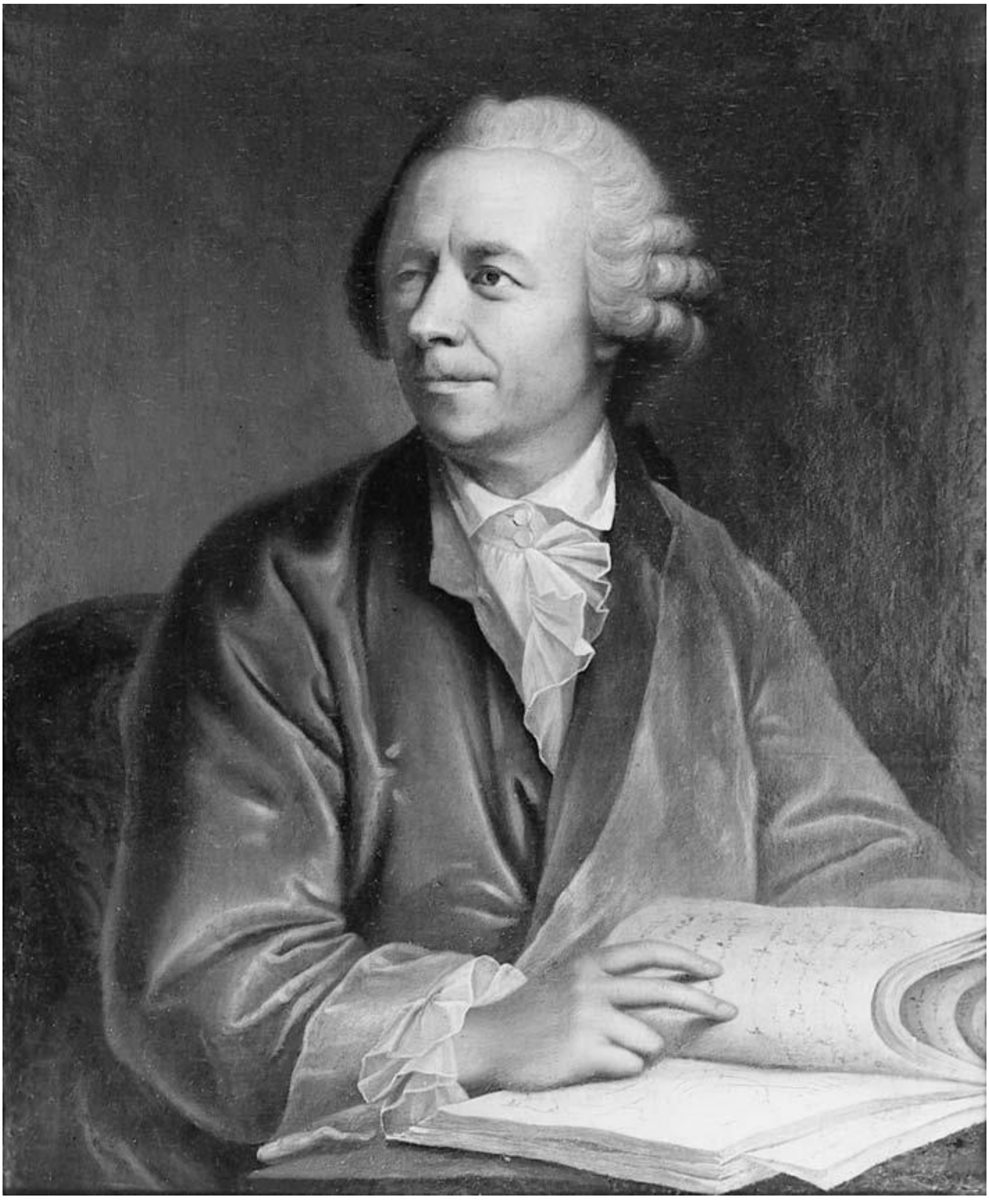
—Classical results
—Schnirelmann density
—Sieve method
—Circle method

Exercices

Open problems……………………………………………………………………..300
bibliography………………………………………………………………………..30

First part

Elementary Theory of Numbers



Lehonard **Euler**

Chapter 1

Recreational number theory

The Greeks were interested in proprieties of integer numbers, to which they often associated religious significations, a subject that historians call *numerology*. It was his not really number theory but number recreation. Names like **Nicomachus**, **Plutarc.**

Their treatment of number with geometric flavor, But lately when combined they are seen as length, area, and volumes of geometrical figures like triangles, square, circles, and volumes… as jewelry was the tiplet

$$x^2 + y^2 = z^2$$

Thus ancient number theory may be seen as a part of geometry, and remained until the Middle Ages , and European mathematicians of the Renaissance like **Viète**(1540-1603), … all saw numbers in algebraic expressions : a as a length and a^2 as an area, which implies that for them the expression "$a^2 + a$" has no sens.

The Greeks studied among others, *triangular* and *pentagonal* numbers. A triangular number t_n is the sum of n first integers

$$t_n = 1 + 2 + \cdots + n = \sum_{k=1}^{k=n} k$$

A triangular number takes this name, from the fact that it form of a triangle's shape.

Fig. The number t_4 by two triangles: rectangle and isosceles.

A *square* number s_n =.number is pentagonal number pg_n takes its name from the shape of a *pentagon*[5] , a pentagonal number is given by the formula

$$pg_n = \frac{n(3n-1)}{2}$$

The first five are

$$1, \quad 5, \quad 12, \quad 22, \quad 35.$$

Between them there is the relation

$$pg_n = t_n + 2t_{n-1}$$

---

[5] A polygon that has 5 sides.

And

$$p_n = t_{n-1} + s_n$$

These all are called $\underline{k - gonal}$ numbers, the nth one is given by the formula

$$\frac{1}{2}k(n^2 - n) - n^2 + 2n$$

In all this, *numbers* are regarded by Greek mathematicians as magic entities and tried to look at them abstractly.

Until the time of **Euclid**, who could to numbers. To feel much their number theory in modern term, we first take a look at integers.

Divisors:

The set of numbers

$$\{\ldots -3, -2, —1, 0, 1, 2, 3 \ldots\}$$

constitute the infinite set of relative integers, or simply integers, a set noted $\mathbb{Z}$. It is a very important set in numbers theory, and known from old[6] times , algebraist and number theorist L. **Kronecker** (1823-1891) said once

God created the integers and all the rest is the work of men

We say that the integer b *divides* the integer a if there exists an integer k such that $a = kb$. We write also $b | a$, and we say that b is a *divisor* of a, and a *multiple* of b. Otherwise if a does not divide b we write $a \nmid b$. The number 1 divides every integer n, it has no great importance.

---

[6] It is to notice that there were English mathematicians at the end of XVIII century that did not accept negative integers.

Example:

For the number $a = 12$, we write

$$4 | 12$$

As $12 = 4 \times 3$ and we have $7 \nmid 12.$

For any two integers a, b we can define two particular integers:

$-$the greatest common divisor (gcd) : or simply (a, b), to find it we use the *factors method.*

$-$the least common multiple $(lmc(a, b)$: also, we may use the method of factors to find it.

We have the relation that enables us to find $lmc(a, b)$ quickly

Theorem:

let a and b two integers, then

$$gcd(a, b) \times lmc(a, b) = ab$$

Proof :

On a a=da and b=db then ab=dab

■

We now add very special divisors of an integer n and our introduction here is simple, to lead the reader softly to more information on primes. We say that a number n is a *prime* if n has for divisors only 1 and n itself. We can write only a finite part of the set of primes

$$2, 3, \dots, 97, \dots, 2^{5671} - 1, \dots$$

Because it is infinite. The number 2 is the only even prime[7] number and 1 is neither prime nor composite even if some mathematicians like **Leibnitz** $(1645-1702)$, Henri **Lebesgue** $(1875-1941)$, Derrick N. **Lehmer**[8] $(1867-1938)$,… consider it as such. Then to be formally precise:

Definition:

An integer n is prime iff it has only *two distinct divisors.*

We can prove that every integer n is the unique product of prime numbers

$$n = {p_1}^{k_1} \times \ldots \times {p_r}^{k_r} = \prod_{i=1}^{i=r} {p_i}^{k_i}$$

Example:

We the number in prime numbers like this

$$99 = 11 \times 3^2 \qquad \text{and} \qquad 100 = 2^2 \times 5^2.$$

the first question is how to find primes, there is a method devised by the Greek **Eratosthenes** $(276-194)$ to exhibit all the prime numbers less than a quantity x, consists in eliminating the prime numbers and theier multiples de tous les numbers entiers

2, 3, ~~4~~, 5, ~~6~~, 7, 8, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~ , …

The numbers that remain non eliminated are the prime numbers

---

[7] When we say : "let p an odd prime" we mean $p > 2$ or $p \neq 2$.

[8] His son Derrick H. **Lehmer** $(1905-1991)$ also was a number theorist.

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \ldots$$

If $gcd(n_1, n_2) = 1$ we say that n_1 et n_2 are *coprime* (we say also *relatively prime*), they have prime number in common, we may also write $(n_1, n_2) = 1$. We see from the above example that

$$(99, 100) = 1$$

If $(n_1, n_2, n_3) = 1$, the numbers n_1, n_2, n_3 are *mutually coprimes.* Integers can be mutually coprime without being two by two coprime like

$$(5, \quad 10, \quad 21) = 1$$

Note that if $n = p_1 \times \ldots \times p_r$ then the number n and

$$p_1 \times \ldots \times p_r - 1 \qquad \text{and} \qquad p_1 \times \ldots \times p_r + 1$$

are three coprime numbers, i.e. they have not common prime factors.

Now on prime divisors:

Theorem :

If $p|ab$ then : $p|a$ or $p|b$

The reader must notice that if p is not prime the theorem is false[9].

Perfect numbers

---

[9] As $8|2 \times 12$ and $9|3 \times 12$.

The Greeks were attracted by number curiosities and number with special proprieties of their divisors. The number of divisors of any integer n , noted $\tau(n)$ (or $d(n)$ too) , is noted as

$$\tau(n) = \sum_{d|n} 1$$

The integer n is also counted, but it is not a *proper* divisor, it is evident that $\forall$ $n \neq 1 : \ \tau(n) \geq 2$.

If we make the sum of all possible divisors of an integer n , we find the *function sum*

$$\sigma(n) = \sum_{d|n} d$$

We remark that the two functions $\tau(n)$, $\sigma(n)$ are written under the form

$$\sum_{d|n} f(d)$$

***Example**:*

$\tau(49) = 3$
$\sigma(49) = 1 + 7 + 7 + 49 = 64$
$\tau(42) = 4$
$\sigma(42) = 1 + 6 + 7 + 42 = 56$

A *perfect* number n is a number that equals to the sum of its proper[10] divisors (n itself is excluded).

---

[10] An old name is "*aliquot parts*" of n.

$$n = \sum_{d|n} d = \sigma(n) - n$$

or simply $\sigma(n) = 2n$. The numbers 6 , 496 and 8128 are the three first perfect numbers. The interest of perfect numbres resides in a historically important theorem which goes back to **Euclid** (*book IX* of the *Elements*):

Theorem :

if $2^n - 1$ is a prime number p , then the number 2^{n-1} $(2^n - 1)$ is an even perfect number .

it is easy to show that if $2^n - 1$ is prime then n is prime itself.

Ancient mathematicians also studied *amicable numbers*, two integer n_1 and n_2 are amicable if

$$\sigma(n_1) = \sigma(n_2)$$

Some rules were confiscated to find them were already known to Greeks also **Thabit** ben **Kurra**(8-8), in

Euler the rules in modern notation in 1747. A was discovered by **Legendre** in 1830.

Bachet theorem

With divisors and primes we have with linear equations. If a and b are coprime then we have an old result in number theoy, namely

Theorem

If $(a, b) = 1$ then there exits two integers x , y such that

$$ax + by = 1$$

and x et y are also coprime .

This sort of results has been given by **Bachet** (1581-1638), **Bézout** (1730-1783) and **Gauss** (1777-184) and belongs to **Diophantine** equations, which we shall see in Chapter 5. Given two coprime integers a and b, we can find x and y like this:

Suppose without loss of generality that $b > a$

From $ax + by = 1$ we get $a(x + y) + cy = 1$ then we have for $k \in \mathbb{Z}$

$$\begin{cases} x + y = k \\ y = \dfrac{1 - ak}{c} \end{cases}$$

by trial and error we can find a solution (x_0, y_0).

Proof :

Suppose that $p \nmid a$ or the same $(p, a) = 1$, then there exists integers x, y such that

$$ax + py = 1$$

Or

$$abx + pby = b$$

Then

$$p(kx + by) = b$$

which gives $p|b$ ■.

Bachet theorem is a special case of more general

$$ax + by = d$$

We can generalize to more than 2 integers

if $p|a_1 \times \ldots \times a_n$, then p divides at least one of $a_1, \ldots, a_n)$

Mathematicians call this theorem ***Euclid**'s first theorem* [see **Hardy**], or ***Euclid**'s lemma* and it goes a more general form

***Euclid**'s lemma*

If $a|bc$ and $(a, b) = 1$ then $a|c$

It is very useful subsequently. This result goes back to **Euclid** in his *Elements* with a false proof, it has been proved for the first time by **Gauss** in 1801 , see[W]. And sometimes it is called *Gauss* theorem.

Euclidian Division:

Named in honor of **Euclid**, the *Euclidian division* of the integer a and b with a *quotient* q and a *rest* r , this is presented by the inequality

$$a = qb + r \qquad \text{with} \qquad 0 \leq r < |b|$$

This form of division is different from the decimal division $\frac{a}{b}$ like the example

$$\frac{13}{7} = 1.8557142 \ldots$$

Which has no interest here, unlike the Euclidian division which is very linked with the study of gcd, lcm, prime numbers,... and it generalization to algebraic numbers as we shall see.

The reader may remark that we wrote $|b|$ because we work in $\mathbb{Z}$,we can for example have $r > a$ like

$$-113 = 4(-27) - 3$$

R here is negative so we add $(-4 + 4)$ to get

$$-113 = 4(-28) + 1$$

The unicity of r and q can be proved. We suppose that $a = q_1 b + r_1$ and $a = q_2 b + r_2$ this gives

$$b(q_2 - q_1) = r_2 - r_1$$

Which means that $b|r_2 - r_1$, but this true only if $r_2 - r_1 = 0$, for we know that $r_2 - r_1 < b$, then we have $r_2 = r_1$ and thus $q_2 = q_1 \blacksquare$

On must insist on the fact that $b > r$ (how many $b's$ does a contain) but it may be that $q > b$.

We can find also the number (a, b) by the ***Euclid** algorithm* which is faster and more practical ,it has for origin the **Euclidian** division $a = bq + r$ by observing that

$$(a, b) = (b, r)$$

A fact proved as follows : from $a = bq_1 + r_1$, a divisor that divides a and b divides also r and a divisor that divides b and r divides also a, then the a, b and r have the same divisors, and the hence the same gcd.

to obtain we like

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + r_2$$

…

$$r_n = r_{n-1}q_{n+1} + 0$$

The number r_1 takes the place of b and the same for the other r_i : every r_i takes the place of r_{i-1} and we notice that

$$(a,b) = (b,r_1) = (r_1,r_2) = \cdots = (r_{n-1},r_n)$$

Euclid's algorithm makes well the difference between q and b in the equation $a = bq + r$.

We can by use of **Euclid** algorithm obtain this theorem on the gcd:

Theorem:

Soit a et b deux entiers, alors il existe deux entier x et y such that

$$ax + by = gcd(a,b)$$

We have seen the theorem when $gcd(a,b) = 1$, it is called **Bezout** theorem

Proof :

On a ■

so the equation

$$ax + by = c$$

has solution (x,y) if $(a,b)|c$. Any common divisor of a and b will divide d too, because d is the product of the common divisors of a and b.

$$a = p_1 \times p_2 \times p_3 \times n \times n$$

and

$$b = p_1 \times p_2 \times p_3 \times n \times n$$

Then $d = p_1 \times p_2 \times p_3$.. and thus $p_1, p_2, p_3 \ldots |d$

Proprieties of divisors:

we have a practical result to calculate $\tau(n)$ and $\sigma(n)$

Theorem

let $n = {p_1}^{k_1} \times \ldots \times {p_r}^{k_r}$, then

$$\tau(n) = (k_1 + 1) \times \ldots \times (k_r + 1)$$

and

$$\sigma(n) = \frac{{p_1}^{k_1+1} - 1}{p_1 - 1} \times \ldots \times \frac{{p_r}^{k_r+1} - 1}{p_r - 1}$$

Proof :

For every p_i there are $k_i + 1$ divisors of the form : ${p_1}^{k_1} \times {p_2}^{k_2} \times \ldots \times {p_r}^{k_r}$, and for $p_1, \ldots, p_r$ there are

$$(k_1 + 1) \times \ldots \times (k_r + 1)$$

divisors. This has **Gauss** p.

For every p_i , the sum of $k_i + 1$ divisors of the form $p_i \times {p_2}^{k_2} \times \ldots \times {p_r}^{k_r}$, and for : $p_1, \ldots, p_r$, we have a product

$$\sigma(n) = \frac{{p_1}^{k_1+1} - 1}{p_1 - 1} \times \ldots \times \frac{{p_r}^{k_r+1} - 1}{p_r - 1}$$

■

So I the case of perfect numbers :

$$\sigma(2^{n-1}(\,2^{n}-1))$$

We can also define also $rad(n)$ the $radical$ o an intger n as the product of its distinct prime divisors

$$rad(n) \;=\prod_{i\neq j} p_i$$

From the Greeks to Fermat :

The French Pierre de **Fermat** (1-16) who was a diplomat, made a lot of speculations on numbers proprieties, and ideas inherited from the Greeks; he may be seen as a continuator of **Diophantius** of Alexandria. The book of *Arithmetica* was printed in 16, and also **Bachet** "Problemes" in 16.. He a lot about numbers

$$x^2+y^2=a$$

Although he made beautiful work in mathematics,

Following **Diphantus** with polynomial equation as : find x and y such that

$$x^2+y^2=65$$

He **Fermat** conjectured more

$$p=x^2+y^2 \Leftrightarrow \; p=4k+1$$

Fermat was also famous of giving statements about integer numbers without proof or with false ones:

i) The numbers $2^{2^n}+1$ noted F_n , are prime for every n (1659 , letter to **Carcavi**), found false by **Euler**(1732) for $n=5$, it is thought that the set of these primes is finite [**Hardy**, 18] .

ii) The equation $x^n + y^n = z^n$ has no positive integer solutions if $n \geq 3$, a problem known as ***Fermat**'s Last Theorem* (FLT) , solved by English **Wiles** and **Taylor** only in 1996 after more than 350 years. Their proof used a very complex mathematical apparatus which is algebraic number theory, it is certain that **Fermat** has made a big error[11].

It is worth noting that a variant form of the reasoning by induction that we have seen and which use a proof in back direction is *the infinite descent* , invented by **Fermat**. **Weil** said about **Pascal** (p.2) :

> *« At one time, **Fermat** cherished to the thought of devoting a whole book to number theory. In another occasion he tried to persuade **Pascal** to book; of course he realized that **Pascal**'s gifts of exposition were far superior to his own. To our great loss, **Pascal** showed no interest »*.

Exercises

1) organize a rectangular number of dots to form a rectangle .

1) show that $\sum_{k=0}^{n}(2k+1)=(n+1)^2$, by two methods . What represents this sum. Draw a square and deduce the result.

1) give the sum of the first n even integers.

1) show that $t_n + t_{n-1}$ is a square s_n (**Nicomachus**)

1) show that $8t_n + 1 = s_{2n+1}$ (**Plutarc**)

1) for every digits a, b and c we have : $\frac{abcabc}{7\times11\times13} = abc$. Where is the trick?

1) Three men went to a judge to 17 camels the first that he owned the 1/2 the second 1/3 the third 1/9 of them. The judge made two observations and solved the problem like this: he added a camel to the herd and gave to every man his share then he took back his camel. What was the two observations?(from Ancient Arabic stories).

---

[11] See **Polka** p.13.

1) show that a pentagonal number : $pg_n = \frac{n}{2}(3n-1)$. (think of the sum of $3k-2$ integers).

1) prove that

$$\frac{1}{2}\sum_{n=1}^{s}\sum_{k=1}^{n} 2k = \frac{s(s+1)(s+2)}{6}$$

It is the sum : $t_1 + \cdots + t_s$.

1) prove **Nicomachus**' identity, for $n \geq 0$

$$\sum_{1}^{n} k^3 = (\sum_{1}^{n} k)^2$$

1) calculate

$$\sum_{k=1000}^{k=2000} k$$

1) prove that $24|6 \times 5^n - 30$, for $n \geq 0$

1) prove that $24|2 \times 7^n + 3 \times 5^n - 5$, for $n \geq 0$

1) prove that $12|(2n+1) \times (2n^2 + 2n)$, for $n \geq 0$

1) prove that for $n \geq 0$

$$\sum_{k=1}^{n} k(k!) = (n+1)! - 1$$

1) prove that for $n \geq 0$

$$\sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$$

1) prove that for $n \geq 0$

$$\sum_{k=1}^{n} k^3 = (\frac{n(n+1)}{2})^2$$

1) find the sum

$$\sum_{k=1}^{n} k(n+1-k)$$

1) prove by induction for $n \geq 1$

$$\frac{a^{n-1}}{a-1} = a^{n-1} + a^{n-2} + \cdots + a + 1$$

1) show that $\forall n \geq 0$ and $a \geq 0 : (1+a)^n \geq 1 + an$ (**Bernoulli**). What about the case : $-1 < a < 0$? , and : $-1 \leq a$?

1) show that : $\frac{(3n)!}{(3!)^n}$ is an integer for n ≥ 0

1) show that : $2^n > n$ for $n \geq 0$.

1) show that : $e^n \geq n + 1$ for $n \geq 0$.

1) devine a propriety of consecutive square numbers.

1) let n_1 and n_2 two consecutive even integers, show that $n_1 n_2 + 1$ is an impair square.

1) let k_1 and k_2 two consecutive odd integers, show that $k_1 k_2 + 1$ is a squared even integer.

1) prove that : $n! \sum_{k=0}^{n} \frac{1}{k!}$ is an integer.

1) show that : $1 + 2 + 4 + \cdots + 2^{n-1} = 2^n - 1$.

1) when is the number 2^n is the sum of two consecutive odd numbers?

1) show that if : $k < n$ and $(k, n) = 1$ then $n | \sum k$.

1) as a special case : prove that if $n = odd$ than

$$n | \sum_{k=1}^{n} k$$

1) we define *__decimal inverse__* of the number 123 as the number 321 . Show that the difference of a number and its decimal inverse is always divided by 9.

1) calculate the first and last sum of digits(*__the digital root__*) for the following number: 72536, 265379110, 1256984003.

1) how can you know that 4 divides an integer without making the division operation ?

1) give $(196, 32)$ by two methods.

1) give $(64,88)$ under the forme $88a + 64b$, a and $b \in \mathbb{Z}$

1) consider the equation $ax + by = 1$. Show that if x and y are coprime then a, b are also coprime.

1) show that also $(a, y) = (b, x) = 1$.

1) is $(a, x) = (b, y) = 1$ necessary ?

1) if $a = da_1$ and $b = db_1$ where $d = gcd(a, b)$, show that $(a, b) = 1$.

1) find x and y for equations:

i) $13x + 7y = 1$ iii) $17x + 7y = 1$
ii) $11x + 8y = 1$ iv) $11x + 6y = 1$

show that there are infinitly many solutions.

1) what about the system

$$\begin{cases} 13x + 7y = 1 \\ 11x + 8y = 1 \end{cases}$$

1) how many divisors has the number 0?

1) find $gcd(24,36,48,132)$. Hint: $gcd(24, \mathrm{gcd}(36, \mathrm{gcd}(48,132)))$, note that the order is not important.

1) find lcm of 57 and 36 , by two methods

1) show that : $lcm(a, b)|c \Longrightarrow c$ is a common multiple of a and b.

1) show that : if $(a, b) = 1$, then $lcm(a, b) = ab$.

1) show that n and $n + 1$ are coprime by two methods.

1) find $lcm(n, n + 1)$.

1) show that two consecutive odd numbers are coprime.

1) give three integers mutually coprime and two by two coprime.

1) can you give three integers mutually coprime and not two by two coprime?

1) can three integers be two by two coprime and not mutually coprime?

1) let the integers d such that $d \nmid n$ and $(n, d) \neq 1$, find the expression and their number for $n = 20$

1) prove that any natural integer n is either of the form ($2k, 2k + 1$) or of the form $(3k, 3k + 1, 3k + 2)$.

1) show that $\frac{n(n^2+2)}{3}$ is an integer.

1) prove that 3 divides one of the numbers $(n, n + 2, n + 4)$

1) show that number primes can have unity 1, 3, 7 or 9

1) find the possible last two digit of a square m.

1) show that 1 is coprime with every integer n

1 show that the only prime de la form $n^2 - 4$ is 5 and $n^3 - 1$ is 7

1) why did we excluded negative primes from our study of integers?

1) show that the square of an odd integer is of the form $8k + 1$.

1) show that if $(n, a) = 1$ and $(n, b) = 1$then $(n, ab) = 1$

1) show this if $(a, b) = 1$, then the same with $(a + b, a)$, $(a + b, b)$ $(a - b, a)$, $(a - b, b)$, $(a^n \pm b^n, a)$, $(a^n \pm b^n, b)$

1) can we write $0 \nmid 0$ as $\frac{0}{0}$ has no sense?

1) let $(a, b, c) = 1$, are the following statements true

i) $a + b|c$

ii) $a - b|c$

iii) $a^2 + b^2|c$

1) show that : if $p|a^n$ then $p|a$.

1) if $a|b$ et $c|d$ then $ac|bd$.

1) if $a|b$ and $b|c$ then $a|c$

1) show that if $a|b$ then $|a| \leq |b|$

1) if in $\mathbb{N}$ $a|b$ and $b|a$ then $a = b$. How would be the equality in $\mathbb{Z}$?

1) show that : if $a|b^k$ then $a|b$ (by first **Euclid**'s theorem)

1) let a and b two integers > 1, show that if $(a, b) = 1$ we cannot have $a^k = b^l$, where k and l are integers > 1.

1) show that if $a = da_1$, $b = db_1$ and $(a, b) = d$ then $(a_1, b_1) = 1$

1) suppose that $n = ab = cd$. Show if : $a > c$ then $b < d$.

1) show that if $2^n - 1$ is a prime then n itself is a prime. Is the converse true?

1) if $2^n - 1$ is prime, calculate $\tau(2^{n-1}(2^n - 1))$.

1) find $\tau(n)$ and $\sigma(n)$ for the numbers:

15, 88, 100, 526, 10236

1) if the divisors of n is only p use geometric series to find $\sigma(n)$.

1) if $\sigma(n) < n$, n is called deficient and if $\sigma(n) > n$ n is called abundant. Give two abundant and two deficient numbers

1) find numbers n such that:

i) $\tau(n) = \sigma(n)$

ii) $\tau(n) > \sigma(n)$

iii) $\tau(n) < \sigma(n)$

1) give n such that $\tau(n) = n$

1) show that $\tau(n) \leq n$
1) show that for $n > 1$: $\tau(n) \geq 2$
1) show that for n even : $\tau(n) \leq \frac{n}{2}$
1) show that for n odd : $\tau(n) \leq \frac{n}{3}$
1) compute : $\tau(\,\tau(\,\tau(100)))$
1) show that : $\tau(\tau(\dots\tau(n))) = 2$
1) suppose that n is excluded from $\sigma(n)$, give n_1 and such that $\sigma(n_1) > n_1$ and another n_2 such that $\sigma(n_2) < n_2$
1) compute : $\sigma(\sigma(\sigma(100)))$
1) calculate $\tau(n)$ and $\sigma(n)$ if $n = p^m$
1) if $n = n_1 \times n_2$ calculate $\sigma(n)$ and $\tau(n)$ what do you remark?
1) calculate : $\lim_{n\to\infty} \frac{\tau(n)}{\sigma(n)}$, (think of $n = p, n = p^m$).
1) calculate the radical of every number: 10, 35, 40, 88, 100
1) is : $rad(n_1 \times n_2) = rad(n_1) \times rad(n_2)$?

Suplementary exercices

1) show that : $e^n \geq n + k$ pour $n \geq k \geq 1$
1) show that : $n^n > n!$ for $n > 2$
1) show that for $n \geq 2$: $n^2 > n + 1$
1) show that : $n! > n^2$ for $n \geq 4$
1) show that : $n\,! > n^3$ for $n \geq 6$
1) compare between $2n^2$ *and* $n^2 + 2n + 1$
1) show that $4n^2 \geq n^2 + 2n + 1$, for $n > 1$ without induction.
1) use **Euclid** theorem to find the first perfect numbers.
1) show that the number d'unities of an even perfect number est toujours 6 or 8.
1) show that $3^n = 2^n + 2r + 1$ where r is an integer.
1) let $n > 1$, prove that 3^n is the sum of three consecutive numbers
1) show that if $(a, b) = 1$ and $ab = c^2$ alors a et b are squares.
1) show that $(am, bm) = m(a, b)$
1) By another method, show that for $n \neq 1$: $(n_1 + n_2)! \neq n_1! + n_2!$
1) show that every perfect number is triangular.

1) show that if $(a,b)=1$ et si $c|a$ et $d|b$ alors $(c,d)=1$

1) show that $\frac{\tau(n)}{n}$ is bounded . is $\lim_{n\longrightarrow\infty}\frac{\tau(n)}{n}=0$?

1) When we evaluate the last sum of digits(the digital root) of a square, we always get either the squares : 1, 4, 9 or the prime 7. For example: the last sum of $1111^2=\ 12345321$ is 25 whose digits' sum is 7. Can you explain this phenomenon?

1) is there integer numbers k,n such that : $k!=n^2$?

Chapter 2

The integers $\mathbb{Z}$

After **Fermat**, came the era of **Euler**. In fact, we cannot imagine today's mathematics without Euler. On the contrary of Fermat, considered as an amateur, famous for his thoughts and observations on integers, **Euler** was a professional mathematician and a research engine. He contributed to almost all scientific domains of his time, developed new ideas and methods, solved the solvable and wrote[12] veritable treatises still in print today. **Laplace** would say to his students

> *" Read **Euler** ! Read **Euler** ! he is the master of all of us"*

Arago[13] said

> *" **Euler** calculated without any apparent effort, like humans breathe, like eagles sustain in the airs "*

---

[12] The project of editing and publishing the writings of **Euler** in different parts of knowledge has begun after his death by his nephew (1718) and today more than 80 volumes have been printed.

[13] François **Arago**(1786-1853) was a French physicist and politician. You find this cote in in his *Collected Works* (2/133) in the biography of scientist **Condorcet** (17-17) (2/133). **Condorcet** was also a phylisopher, he wrote in 178 an eulogy preface of **Eulers'** book *Institutiones* saying p.: "he stoped to calculate and live". He died in prison during the French revolution.

H. **Edwards** wrote [p.39]

> *"It is a measure of Euler's greatness that when one is studying number theory one has the impression that Euler was primarily interested in number theory, but when one studies divergent series one fells that divergent series was his main interest, when one studies differential equations one imagines that actually differential equations was his favorite subject… "*

His book *Algebra (1770)* contained the developments of number theory after the era of Diophantus' *Arthmetica*, enriched by his proper contributions, he also had the task of proving the assertions of **Fermat**. **Gauss** had made a remark about that:

> *Higher arithmetic has its special feature that many of its most beautiful theorems may be easily discovered by induction, while any proof can be only obtained with the utmost difficulty. Thus, it was the great merits of **Euler** to have proved several of Fermat's theorems which he obtained, it appears, by induction*[14].

Following the research of the Greek, he proved in 1775 that if n is a triangular number then

$$9n+1, \qquad 25n+3, \qquad 49n+6$$

are also triangular. **Gauss** in 1801, in his big book *Disquisitiones*, art.293, proved an **Fermat** assertion every number n is the sum of three triangular number

he proved that x by **Fermat**

$$p = x^2 + y^2 \Leftrightarrow\ p = 4k + 1$$

---

[14] [**Ribenboim**].

In their quest of numbers' proprieties, number theorists usually make conjectures, and the quest for those conjectures proofs has much developed mathematics. To prove, they use classical methods that one must master and use without fear.

Methods of proof:

In order to prove proprieties on integer numbers one must first have the definitions, and a definition is a very important in the of any proof. Then he use always one of the following demarches :

a) Find a counter-example

Example:

To prove that the statement $(n_1 + n_2)! = n_1! + n_2!$ is false for positive $n > 1$, we can find a counter-example

$$(2+3)\,! = 120 \ \neq \ 2! + 3\,! = 8$$

■

b) Prove directly by either an elementary, algebraic or analytic method

$$A \Longrightarrow B$$

read " if A then B ".

Example:

Show that the number $(n+1) \times (3n+2) \times (3n+1)$ is always divisible by 2.

If n is even then 2 divides $3n+2$, and if n is odd then 2 divides $n+1$■

c) Proof by contraposition

$$A \Longrightarrow B \Leftrightarrow \neg B \Longrightarrow \neg A$$

It is usually easier to proof a propriety by contraposition.

Example:

Show that

r■

d) Proof by *reducto ad absurdum*,

$$(\neg A \Longrightarrow B) \wedge (\neg A \Longrightarrow \neg B) \Longrightarrow A$$

or

$$(\neg A \Longrightarrow \perp) \Longrightarrow A$$

Which means that to prove A we suppose that A is false and we get to a contradiction. Or to prove A is false, we suppose that A is true and we get to a contradiction.

Example:

let us prove that

$$1 = \frac{1}{a_1} + \cdots + \frac{1}{a_k}$$

Cannot be true if k is even and a_i are odd. Suppose that the statement is true , then by addition we get a fraction with an odd nominator an even dominator, a contradiction.■

e) Proof by induction, in*duction* is one of the essential proprieties of the sequence of integers. We can prove much of the known results on the integer numbers by using *induction*, whose uses go beyond number theory.

Definition of the Principle of induction :

If the propriety P is true for the number n , then it is true for $n+1$ or

$$P_n \Longrightarrow P_{n+1}$$

The first use of this principle goes back to French mathematician Blaise **Pascal** (16-16) in his book "*Treatise of the Arithmetic Triangle* " (1653).

Example:

prove by induction that for every $n \geq 1$ we have :

$$1+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$$

We see that the propriety P_n is true for $n=1$ qui est vraie : $1=1$. We suppose now that P_n est vrai pour n (par exemple $n=1$) et on le prouve pour $n+1$. We have then

$$1+2^2+\cdots+n^2+(n+1)^2=\frac{n(n+1)(2n+1)}{6}+(n+1)^2$$

$$=\frac{(n+1)(n+2)(2n+3)}{6}$$

so $P_n \Longrightarrow P_{n+1}$

which proves the propriety■.

Return to perfect numbers

Euler explored perfect numbers. The numbers 2^p-1 have become important for mathematicians in their search for perfect numbers. They are named *Mersenne numbers* M_p ,in honor of French **Mersenne**(1588-1648) who studied them around 1644, the greatest known M_p is

$$2^{77232947} - 1$$, (S 2017)

Afterwards, and in 1755, **Euler** proved the following theorem stated previously by **Descartes**.

Theorem:

Every even perfect numbers is of the form $2^{n-1}(2^n - 1)$.

It is the converse of theorem 5, which give us an equivalence or a sufficient and necessary condition :

i) if $2^p - 1$ is a prime $\Longrightarrow$ $2^{p-1}(2^p - 1)$ is an even perfect number.

ii) if $2n$ is a perfect number $\Longrightarrow$ $2n = 2^{p-1}(2^p - 1)$, and $2^p - 1$ is prime

We do not know yet, if there exists an *odd* perfect number . But we know well that the first in the list would be very big. In fact , if N_{im} is the first odd perfect number then

$$N_{im} > 10^{1500}$$

Euler's function $\varphi(n)$:

Called also *indicator*, *phi* function or *totient*[15]. Noted $\varphi(n)$, it is equal to the number of integers coprime with n.

$$\varphi(n) := \{\#\ m : m < n\ and\ \ (n, m) = 1\}$$

---

[15] A word coined by English number theorist **Sylvester**(18-1).

with φ[16]$(1) = 1$, or

$$\varphi(n) \; = \sum_{(n,m)=1 \;\wedge\; m<n} 1$$

The function φ is the first *arithmetic function* introduced by **Euler**, we will see more such functions. He also has given us a formula that computes it:

Theorem

If : $n = {p_1}^{k_1} \times \ldots \times {p_k}^{k_r}$ then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \times \ldots \times \left(1 - \frac{1}{p_k}\right)$$

Notice that if we consider 1 as a prime the formula gives 0.

Example :

$$\varphi(10) = 10 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 10 \times \frac{1}{2} \times \frac{4}{5} = 4$$

These 4 number are: $1, 3, 7{,}9$. We prime only once, so

$$\varphi(9) = 9 \times \left(1 - \frac{1}{3}\right) = 9 \times \frac{2}{3} = 6$$

Those 6 number are: $1, 2, 4{,}5{,}7{,}8$.

The notation $\varphi(n)$ is due to **Gauss**, who could prove the following:

---

[16] " the number $\varphi(1)$ is in itself without meaning, but by special definition one puts $\varphi(1) = 1$" , [**Ore**].

Theorem:

For every positive integer n

$$n = \sum_{d|n} \varphi(d)$$

Proof :

■.

The function φ is an example of *arithmetic* function we will discover many other important in number theory.

Example :

$$10 = \varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4$$

If $n = n_1 \times n_2$ and $(n_1, n_2) = 1$ then

$$\varphi(n_1 \times n_2) = \varphi(n_1) \times \varphi(n_2)$$

a very important propriety which we will see later.

Fraction

If $a \nmid b$ then $\frac{b}{a}$ is not an integer and is compsed of an integer $[\frac{b}{a}]$ and a decimal part noted $\{\frac{b}{a}\}$

$$\frac{b}{a} = \left[\frac{b}{a}\right] + \{\frac{b}{a}\}$$

We can generalize these two notions, in general if $x \in \mathbb{R}$, we note by $[x]$ the greatest integer $n \leq x$ and by $\{ x \}$ its decimal part.

Example:

For the number $a = 1.212121$, we write

$$[a] = 1 \qquad \text{and} \qquad \{a\} = 0.212121$$

also we have

$$[-3] = -4 \qquad \text{and} \qquad \{-4.231\} = -0.231.$$

These two concepts are not at all trivial, for we find them in some formulas such as ***Euler's*** *constant*

$$\gamma = \int_{1}^{+\infty} \frac{\{x\}}{x^2} dx$$

and in ***Tchebechev's*** *function*

$$\psi(x) = \sum_{p \le x} \left[\frac{logp}{logx} \right] logp$$

Some mathematicians use the symbol $\left\lfloor \frac{b}{a} \right\rfloor$ for the greatest integer $< \frac{b}{a}$ and the symbol $\left\lceil \frac{b}{a} \right\rceil$ for the least integer $> \frac{b}{a}$, and we have

$$\left\lfloor \frac{b}{a} \right\rfloor \le \frac{b}{a} \le \left\lceil \frac{b}{a} \right\rceil$$

Example:

$$\left\lfloor \frac{5}{2} \right\rfloor = 2 \quad \text{and} \quad \left\lceil \frac{5}{2} \right\rceil = 3.$$

More on primes:

We return now to prime numbers,

Theorem :

the set of prime number $\mathbb{P}$ is infinite.

This result first by **Euclid** in his the *Elements*.

Fundamental theorem of arithmetic :

let n be an integer , then we can write it as a product of distinct numbers premiers .

$$n = \prod_{i=1}^{i=n} {p_i}^{k_i}$$

This result goes back to **Euclid** in his *Elements*. Evident, it has been proved for the first time by **Gauss** in 1801.

Proof :

if n is prime we have nothing to do $(n = p)$, if not then n has divisors we take the least one p_1 so we have $p_1|n$ and $n = p_1 n_1$ the p_1 should be prime otherwise we have a

$$0 < d < p_1 \quad \text{and} \quad d|n$$

contradiction, we do the same with n_1 as with n and so on until we find all the p_i

$$n = {p_1}^{r_1} \times \ldots \times {p_k}^{r_k}$$

■

for unicity , suppose that n has two different products of primes

$$n = {p_1}^{r_1} \times \ldots \times {p_k}^{r_k} = {q_1}^{s} \times \ldots \times {q_j}^{s}$$

Then $\forall p_i \quad p_i | {q_1}^{r_1} \times \ldots \times {q_j}^{r_k} \quad \Longrightarrow \quad p_i | q_i \Longrightarrow \quad p_i = q_i$ ■

Remark that if we consider the number 1 as a prime, the theorem is false for the decomposition would not be unique:

$$n = 1 \times p_1 \times \ldots \times p_n = 1 \times 1 \times p_1 \times \ldots \times p_n = \ldots$$

we will learn subsequently, that prime numbers are a fountain of problems and conjectures in number theory .we discuss prime numbers more in subsequent chapters.

Exercises

1) show that 3 consecutive integers is divisible by 3(generalize).
1) show that $n^4 - n^2$ consecutive integers is divisible by 3.
1) show that 3 consecutive integers is divisible by 6.
1) prove by induction that

$$t_n = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

draw a triangle and derive the formula. Give **Gauss**'s solution.

1) Euler thought that M_{41} and M_{47} were prime, show that they are composite.

1) show that $\varphi(n)$ is even for $n > 2$.

1)calculate $\varphi(0)$, why does $\varphi(1)$ meaningless? Why did we put $\varphi(1) = 1$?

1) give : $\varphi(n)$ pour $1 \leq n \leq 20$

1) find n such that $\varphi(2n) = n$, and another n: $\varphi(n) = \varphi(2n)$

1) when are n and $\varphi(n)$ coprime ?

1) are there infinitely many n such that : $gcd(\varphi(n), n) > 1$?

1) show that if : $k|n$ then $\varphi(k)|\varphi(n)$

1) show that in the equation $a = qb + r$: r is unique $\Leftrightarrow$ q is unique.

1) consider the equation $a = qb + r$ when $a = -13$ and $b = 3$. Show that there are infinitly many integers q , r that verify the equation . Give their values in the case of **Euclidian** division.

1) show that : $q = \left[\frac{a}{b}\right]$

1) give a counter-example to the two assertions :

$[x_1 + \cdots + x_n] = [x_1] + \cdots + [x_n]$

$[x_1 \times \ldots \times x_n] = [x_1] \times \ldots \times [x_n]$

1) prove that : $[x_1 + x_2] \geq [x_1] + [x_2]$

1) prove that :

i) $[x] \leq x < [x] + 1$

ii) $[x] - 1 \leq x < [x]$

1) show that $\forall x \in \mathbb{R}$: $x - [x] \geq 0$

1) let $p_1, \ldots, p_n$ be the first n primes, show that

$$\prod_{k=1}^{k=n} p_k\left(1 - \frac{p_{k-1}}{p_k}\right) > 2^{n-1}$$

1) show that if $p|a$ et $p|b$ alors $p|a + b$ et $p|a - b$

1) show that if $p|a$ and $p|b$ alors $p|am + bn$

1) is it true that if $p|(a + b)$ then $p|a$ or $p|b$?

1) show that for every prime $p > 5$, $p^2 + 2$ cannot be prime.

1) show that for every prime $p > 2$, $p^2 + 1$ cannot be prime.

1) que p prime, the numbers $p, p + 2, p + 4$ cannot be all prime

1) there is no prime of the form $n^4 + 4$ for $n > 1$.

1) show that a progression $ak + b$ cannot contain primes only.

1) show that every prime is of the form $2k_1 + 3k_2$ $/ k_1, k_2 \in \mathbb{N}$

1) show that every prime $p \geq 3$: $p = 3n + 1$ or $p = 3n - 1$

1) show that every prime $p \geq 3$: $p = 4n + 1$ or $p = 4n + 3$

1) show that all primes $p > 5$ are of the form $6n + 1$ or $6n - 1$ (**Euclid**).

1) let $n = p_1 \times \ldots \times p_k$, show that : $\sqrt[k]{n} \leq \max(p_1, \ldots, p_k)$.

1) show that at least one of the p_i is $\leq \sqrt{n}$. at most one $> \sqrt{n}$.

Chapter 2

Congruences

The theory of congruence is a very useful and fecund reformulation of classical theory of divisibility. This branch today is known under the name of :
'' *modular arithmetic* [17]'' .
To simplify the problems of divisibility in $\mathbb{Z}$ and the language of number theory in general, we use the marvelous idea of congruence introduced by **Gauss** in 1801, in his big book *Arithmetic Researches* or in Latin *Disquisitiones Arithmeticae*. This great book has been written by **Gauss** when he was 24 years old.

Disquisitiones is a book articles they are 366 articles. In it proved a lot of result and original ones.

3) Residues modulo an integer n :

Definition :

---

[17] Modular from modulo and arithmetic is the sciences of numbers in contrast of algebra the science of searching for number solutions using letters as unknowns.

We say that the integer $a \in \mathbb{Z}$ is *congruo to the integer b modulo the integer n* if $a = kn + b$, and we write

$$a \equiv b \ mod \ n$$

The number n is called the *modulos*, a Latin word used by **Gauss** meaning *measure* , so the notation $a \equiv b \ mod \ n$ means

a is equivalent to b by the measure "n"

the number b which we have named *the rest* in **Euclidian** division has become *the residue*. If a is a multiple of n then we write

$$a \equiv 0 \ mod \ n$$

Examples :

$$8 \equiv 3 \ mod \ 5$$

and

$$9 \equiv -7 \ mod \ 4$$

and

$$81 \equiv 0 \ mod \ 9$$

Gauss in his book *(Work ,vol. 1, p. 10)* gave two examples

$-16 \equiv 9 \ mod \ 5$ and $-7 \equiv 15 \ mod \ 11$

This formulation make the divides the set $\mathbb{Z}$ into *classes of equivalence*, noted

$$\dot{0}, \dot{1}, \dot{2}, \dots, (n \dot{-} 1)$$

If $n = 4$, the possible classes (of residues) are

$$\dot{0}, \dot{1}, \dot{2}, \dot{3}$$

Which gives : $15 \in \dot{1}$ and $100 \in \dot{0}$… for $15 \equiv 1 \; mod \; 4$ and $100 \equiv 0 \; mod \; 4$

Here are some proprieties that are easy to prove:

Theorem :

If we have : $a \equiv b \; mod \; n$ then

i) $b \equiv a \; mod \; n$
ii) $a + k \equiv b + k \; mod \; n$
iii) $ak \equiv bk \; mod \; n$
iv) $a^k \equiv b^k \; mod \; n$

Complete system of residues

Let n be an integer, the classes $\dot{0}, \dot{1} \dots, (n \dot{-} 1)$ are a *complete system of residues*, for $n = 7$ the complet is

$$1, \dot{2}, \dot{3}, \dot{4}, \dot{5}, \dot{6}$$

if we take only the classes relatively prime to n we obtain a *reduced system of residues* which contains $\varphi(n)$ elements , as an example $n = 6$ we have

$$\dot{1},\dot{5}$$

Theorem:

Let n and 1,… r its reduced class stem then

$$\sum_{i1} r_i \equiv 0\ mod\ n$$

To integer numbers we can also deal with polynomials, for polynomials **Gauss** asked to find integer x such that

$$ax + c \equiv b\ mod\ n$$

or

$$ax \equiv b - c\ \ mod\ n$$

that is equivalent to the linear equation

$$ax + ny = d\ ,\ (d = b - c)$$

It has been observed that these cases could be se reduced to one case : when $n = p$ is a prime, to get rid of the problems $(a, n) \neq 1$ and $a|n$

$$ax \equiv b - c\ \ mod\ p$$

For if $a = nk + b$ then $a = pr + b$ it is equation general and easy to. We see that ere not always a solution , for example the equation $ax \equiv b\ \ mod\ p$ has no solution n a alors

Theorem:

The equation

$$ax \equiv b \bmod n$$

has a solution if $a \nmid n$.

Higher power residues:

Gauss considered also les *quadratic* equations : trouver les entiers x such that

$$ax^2 + bx + c \equiv d \bmod k$$

It suffices to consider the case

$$x^2 \equiv n \bmod p$$

The reader will notice the is more interesting if take the general congruence

$$a^k \equiv b \bmod n$$

Why? Because b will take different values and the questions are

Questions:

i) can b take infinitely many values? if no, how many?

ii) it is obvious that k has periods, what periods?

iii) what value may and may not take ?

iv) may b take the value 1?

The first questions is easy : no, b may take a finite , it is obvious that the number of the values $< n$.
The forth question set by **Euler**

Theorem of **Euler**(1760) :

If $(a, n) = 1$, then on a

$$a^{\varphi(\mathrm{n})} \equiv 1 \; mod \; n$$

In our study of residues, It is natural after linear equation, to begin by the quadratic exponent. We say that a the integer n is a *quadratic residue modulo p* if $p \nmid n$ and

$$x^2 \equiv n \; mod \; p$$

We have an answer to the question i):

Theorem:

the number of residus of the equation $x^2 \equiv n \; mod \; p$ is $\frac{p+1}{2}$

These residues are called quadratic residues modul p , for example the possible quadratic residues modulo e folowing primes are underlined:

2 :

3 :

5 :

7 :

9 :

11 :

13 :

17 :

19 :

To ask naturally:

Questions:

i) for a given intger n , what are les numbers premiers p pour qui n est un résidu quadratique (n'est pas un résidu quadratique)?

ii) for a given prime p quels sont les entiers n qui sont résidu quadratiques (ne sont pas des résidus quadratiques)?

The equation $x^2 \equiv n \ mod \ p$ se réduit aussi aux premiers impairs $p \ et \ q$

$$x^2 \equiv q \ mod \ p$$

On dit comme auparavant : q est dit *quadratic residue modulo* p. Une question se pose :

— Soit p an odd prime, quel sont les q qui sont des résidus ou non résidu modulo p ?

— Inversement soit q an odd prime quels sont les values de q pour qui p est un résidu quadratique ?

Ces deux questions vont être traitées in the *law of reciprocity*.

it is easy by the use of congruences solve equations of the form : quel est le reste b de la division de a^n par d , écrit autrement

$$a^n \equiv b \ mod \ d$$

Example :

quel est le reste of division number 11^{999} by 3 ? on fait la congruence

$$11 \equiv 2 \equiv -1 \; mod \; 3$$

then

$$11^{999} \equiv (-1)^{999} \equiv -1 \; mod \; 3$$

The rest is 2.

Primitive roots:

We now look at an important needed for the subsequent chapters.

-it is obvious that k has periods what periods?

Dans des existe l des solutions of equation

$$a^k \equiv 1 \; mod \; n$$

Alors ce qui nous amène à la definition

Order of an integer a modulo n

Definition:

Let $(a, n) = 1$, we say that k is the order of a *modulo n* if

$$a^k \equiv 1 \; mod \; n$$

Remark that the if $(a, n) = 1$ otherwise the solution. is impossible

We return to the function $\varphi(n)$

Definition:

Let $(a, n) = 1$, we say that a is a *primitive* root *modulo n* if a is of order $\varphi(n)$ modulo n.

-what value may and may not take ?

Definition :

Let n >1, we say that a is a *primitive root modulo n* if there exists a k such that

$$a^k \equiv b \bmod n \quad , \quad (n, b) = 1$$

or if

$$a^{\varphi(n)} \equiv 1 \bmod d \quad \text{et} \quad a^{\varphi(n)} \not\equiv 1 \bmod d \qquad [\text{ for} < \varphi(n)].$$

Pour bien on prend $n = p$, alors on dit que a est une $racine\ primitive\ modulo\ p$ if

$$a^{p-1} \equiv 1 \ (modulo\ p)$$

ou

$$a^q \equiv 1 \bmod p \quad \text{for} \quad 1 \leq q < p - 1$$

Example :

The number 2 is a primtive root modulo 5 car on a bien

$$2^1 \equiv 2 \bmod 5$$

$$2^2 \equiv 4 \bmod 5$$

$$2^3 \equiv 3 \, mod \, 5$$

$$2^4 \equiv 1 \, mod \, 5$$

the numbers copreme with 5 are indeed 4 numbers : 1, 2, 3 and 4 , which is the number $\varphi(5)$, then 2 is a primitive root modulo 5.
Euler was the first à dégager this concept and gave the word *primitive root*. In 1769 , Lambert conjectured que pour tout $premier \ p$ il existe des racines primitives modulo n, un résultat que **Euler** démontra en 1773. **Gauss** showed that for every prime p il existe des racines primitives. Il a aussi conjectured there are infinitey de premiers ayant la racine primitive 10.
in 1927 **Artin** a generalized the conjecture : if a est différent de 1 et -1 , existe-an infinity of primes having the primitive root a? a conjecture qui n'est pas encore résolu.

Reciprocity law

before entering in the celebrated reciprocity laws we must Fermat chercha a trouvé si un p une équation quadratique

$$ax^2 + bx + c$$

On a vu that in general on dit que n est un quadratic résidue of p (or modulo p) si $p \nmid n$ et $x^2 \equiv n \, mod \, p$.

Then Euler his Euler criterion, the first who gave a to it by mathematicians. in 1748 **Euler** for when the rest division of square x^2 when p is a by notation

$$x^2 \equiv a \, mod \, p$$

is a or not he eumer criterion: if a est différent de 1 et -1 .

Definition:

Let n >1, we say that a is a *quadratic residue modulo p* then :

$$a^{\frac{p-1}{2}} \equiv 1\, mod\, p$$

or if

$$a^{\frac{p-1}{2}} \equiv -1\, mod\, p$$

this the departure for the laws of reciprocity that will I XIX century this will be written by **Legendre** as

$$\left(\frac{a}{q}\right)$$

Examples:

For $a = 2$ we some primes:

- $2^{\frac{3-1}{2}} \equiv -1\, mod\; 3$, then 2 is not a quadratic residue modulo 3.
- $2^{\frac{5-1}{2}} \equiv -1\, mod\; 5$, then 2 is not a quadratic residue modulo 5.
- $2^{\frac{7-1}{2}} \equiv 1\, mod\; 7$, then 2 is a quadratic residue modulo 7.
- $2^{\frac{11-1}{2}} \equiv -1\, mod\; 11$, then 2 is not a quadratic residue modulo 11.
- $2^{\frac{13-1}{2}} \equiv mod\; 13$, then 2 is not a quadratic residue modulo 3.

Afterwards **Euler** conjectured there is a relation between p est q , more precisely :

$i)$ if $p \equiv$ 1 modulo 4 : $x^2 \equiv\; p\, mod\, q \;\Longrightarrow\; x^2 \equiv q$ mod p

$ii)$ if $p \equiv$ 1 modulo 4 : $x^2 \not\equiv$ $p$modulo q $\Longrightarrow$ $x^2 \not\equiv$ $p$mod q.

And

$i)$ if p et $q \equiv 3 \bmod 4$: $p \equiv x^2\ mod\ q \implies q \equiv x^2\ \ mod\ p$

$ii)$ if $p \equiv 3 \bmod 4$: $p \not\equiv x^2 \bmod q \implies q \not\equiv x^2 \bmod p$

And discovered a criteria to this phenomenon

$$a^{\frac{p-1}{2}} = \begin{cases} 1 if\ \ p\ est\ un\ residu\ quadratique\ modulo\ q \\ \qquad\qquad\qquad 1\ if \end{cases}$$

in his attempts to prove this result, **Legendre** reformulated observation of **Euler** and introduced his notation $\left(\frac{a}{p}\right)$:

$$\left(\frac{a}{q}\right) = \begin{cases} \quad 1\ si\ a\ est\ un\ residu\ quadratique\ modulo\ p \\ -1\ si\ a\ n'est\ pas\ un\ residu\ quadratique\ modulo\ p \end{cases}$$

$i)$ si $p \equiv q \equiv 1$ modulo 4 alors $x^2 \equiv p$ modulo q ssi $x^2 \equiv q$ mod p

$ii)$ si $p \equiv q \equiv -1$ modulo 4 alors $p \equiv x^2$ modulo q ssi $q \not\equiv x^2$ mod p

Legendre (1798) coined the expression *law of reciprocity*,

The law of reciprocity become with the symbol of **Legendre**

Legendre's definition

Soit un premier $p \neq 2$ et un entier a impaire alors

$$\left(\frac{p}{a}\right) = (-1)^{(p-1)(a-1)/4}$$

Example :

the number 3 is a quadratic résidu of 5 for

$$\left(\frac{3}{5}\right) = (-1)^{(3-1)(5-1)/4} = +1$$

the number 2 is not a quadratic résidu of 5 for

$$\left(\frac{2}{5}\right) = (-1)^{(2-1)(5-1)/4} = -1$$

The first proof of the reciprocity law is due to Gauss in 1796 . Gauss saw it as qui le *fundamental theorem* and the *golden theorem*, and he formulated thus :

– if $p \equiv 1$ modulo 4 then $p \equiv x^2$ modulo q ssi $q \equiv x^2$ mod p

– if $p \equiv -1$ modulo 4 then $q \equiv x^2$ modulo p ssi $-p \equiv x^2$ mod q

Or the same : if p and q sont des premiers impaires alors

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) \; si\; q \equiv 1 \; mod\; 4 \; ou \; p \equiv 1\, mod 4 \\ -\left(\frac{q}{p}\right) \; si\; p \equiv 3\, mod\; 4 \; ou \; q \equiv 3\, mod\; 4 \\ 0 \; si\; q|p \end{cases}$$

Gauss gave another three proofs of the reciprocity la. aussi attaqua le cas $= 3$ the first proof is due to Eisenstein in 1844. Puis il attaque la loi *biquadratique* :

$$x^4 \equiv q\; mod\; p$$

Mathematicians of XIX century attaquait other exponents mais il restait à trouver le cas général

$$x^n \equiv q\; mod\; p$$

Jacobi attaqua le problème et introduit *le symbole de Jacobi* une généralisation du symbole de **Legendre**

Definition (**Jacobi** 1837)

$$(n|P)= \prod_{i=1}^{i=n} \left(\frac{n}{q_i}\right)$$

called symbole of **Jacobi**.

where $P = \prod_{i=1}^{i=n} q_i$ and $\left(\frac{n}{q}\right)$ is the **Legendre** symbol, Le de **Jacobi** facilita les calculs

Example [2] :

the number 104 est un quadratic residue modulo 997

$$104 = 24 = -1$$

then

$$(104|997) = (104|997) = -1$$

so 104 is a quadratic residue of 997.

Reciprocity laws are very important dans la theory des congruence , quadratic forms , factorization,… it has more than 200 proofs dont ceux de Gauss, Cauchy, Jacobi, Dirichlet, Kronecker… voir[].

The great generalisation est de cette loi est *Hilbert's ninth problem* : la loi de réciprocité dans les corps de nombres qui trouve sa solution partielle dans la théorie des corps de classes (Artin, Hasse, Takagi, …).

Chinese remainder theorem

un famous theorem dit theorem is a result on divisibility it is better to treat it by the theory of congruence

Theorem:

Let $n_1, \dots, n_k$ sont premiers entre eux then there exist a nautral i n such that et

$$n_1 \equiv a\, mod\ \ , \dots, n_k \equiv a\, mod$$

And $1 < a_i < n_i$.

The Chinese origin of his problem is practical in the

Example [2] :

Le number 4, 5, 7 and we have n

$$n_1 \equiv a\, mod$$

$$n_1 \equiv a\, mod$$

$$n_1 \equiv a\, mod$$

Exercises

1) find the missing numbers:

i) $-7 \equiv\ .\ mod\ 17$

ii) $8 \equiv .\ mod\ 15$

iii) $-11 \equiv .\ mod\ 9$

iv) $5 \equiv\ .\ mod - 9$

1) Show that

$i)$ $a \equiv b \; mod \; n$ alors $a - b \equiv 0 \; mod \; n$
$ii)$ $a \equiv a \; mod \; n$
$iii)$ $a \equiv b$ mod n $\Longrightarrow b \equiv a \; mod \; n$
$iv)$ $a \equiv b \; mod \; n$ and $b \equiv c \; mod \; n \Longrightarrow a \equiv c$ mod n
$v)$ $a \equiv b \; mod \; n$ and $c \equiv d \; mod \; n \Longrightarrow ac \equiv bd$ mod n. is the reciprocal e true ?
$vi)$ $a \equiv b \; mod \; n$ et $c \equiv d \; mod \; n \;\; \Longrightarrow \;\; a + c \equiv b + d \; mod \; n$
$vii)$ $a \equiv b \; mod \; n$ alors $a + c \equiv b + c \; mod \; n$
$viii)$ $a \equiv b \; mod \; n$ alors $ac \equiv bc \; mod \; n$. Is the reciprocal true ? when is it true? Think of : $3 \times 2 \equiv 1 \times 2 \; mod \; 4$ and $8 \times 2 \equiv 1 \times 2 \; mod \; 7$
$ix)$ $a \equiv b \; mod \; n$ then $a^k \equiv b^k \; mod \; n$, for $k \geq 0$

2) let n_1 et n_2 two integer numbers, show that : $n_1 \equiv r$ mod n_2, a un nombre fini de résidus (rests)

1) show that : if n is a square then : $n \equiv 0 \; mod \; 4 \;\; or \; n \equiv 1 \; mod \; 4$

1) find the solutions : $5x \equiv 1 mod \; 7$

1) find the solutions : $10x \equiv 8 \; mod \; 9$

1) show that the equation : $2x \equiv 3 \; mod \; 4$, has no solutions

1) find x such that : $7^{111} \equiv x \; mod \; 8$

1) show that : $3^{3n+1} + 2^{n+1}$ is divisible by 5 , by two methods.

1) show that : $n^{n-1} \equiv 1 \; mod \; (n-1)$.

1) prove that $(a+b)^p = a^p + b^p mod(p)$. generalize for n terms.

1) prove that : $\dot{0}, \dot{1} \dots, (\dot{p - 1})$ are a complete system of residues.

1) for which value is the complete residue equivalent to the reduced residues.

1) prove that : $ax \equiv 1 \; mod \; b$ has solutions only if $(a, b) = 1$

1) prove that : if $(a, k) \neq 1$ then $a^k \equiv 1 \; mod \; b$ has solutions .

1) why did we in the reciprocity law took $p, q \; \neq 2$?

1) show that 3 is a quadratic residue mod 5 and 2 is not.

1) let $a = 5036$, $b = 1754$ and $c = 2074$. What is the rest of division of $(ac)^{1754} + (bc)^{5036}$ by 3 ?

1) give the order of the following integers modulo n
$i)$ 2,3,6,4,5 : modulo 3
$ii)$ 3,5,8 : modulo 5
$iii)$ 6,7,8 : modulo 7

1) let $13x + 9y = 1$. Show that if (x, y) is a solution then $x \equiv 7 \; mod \; 9$.

1) show that for $n \geq 3$: $n^{n-1} \equiv 1 \; mod \; (n-1)$.

1) verify $\left(\frac{a}{p}\right)$ for $p = 11$ and $a = 2,3,4,5,6,7,8,9,10$.

1) verify $\left(\frac{p}{q}\right)$ for (p, q) : (3,5) , (3,7) , (3,11).

Chapter 3

Properties of primes

One of the ancient results in number theory, was the existence of infinity many prime number in $\mathbb{Z}$.

Euclid second theorem:

We note by $\pi(x)$, the number of prime numbers less than x

$$\pi(x) := \{\# \, p_i \, : \, p_i \leq x\}$$

We write equivalently

$$\lim_{x \to +\infty} \pi(x) \ = +\infty$$

which is the following result, known as *Euclid's second theorem*, if we not the set of prime numbers by $\mathbb{P}$

Theorem:

The set $\mathbb{P}$ is infinite.

Proof:

Suppose that there exist a last prime number p_l , then we consider the integer s

$$s = (2 \times 3 \times 5 \times \ldots \times p_l) + 1$$

if s is aprime we get a contradiction (for $s > p_l$), if s is not prime then it is written as a product of primes

$$s = 2 \times 3 \times 5 \times \ldots \times p_e$$

otherwise there existe another prime $p_e > p_l$ that is not in the list such that $p_e | s$, a contradiction[18]■.

Euler(1737) made another proof which opened the door to analytic number theory, by introduction his product named: ***Eulerian** product*

$$\sum_{n \geq 1} \frac{1}{n^x} = \prod_p (1 - \frac{1}{p^x})^{-1}$$

Qui une relation entre la suite des entiers and the sequence of primes:

$$\lim_{\substack{x \to 1 \\ >}} \sum_{n \geq 1} \frac{1}{n^x} = +\infty$$

---

[18] Ses **Ingham**, p.1 for an interesting argument.

this implies an infinity of prime numbers. Or we can tire precisely that the series of inverse des premier diverges

$$\sum_{p} \frac{1}{p_n} = +\infty$$

which again implies that exist an infinity of primes.

Styding **Mersenne** numbers $2^p - 1$, Fermat discovered his little *theorem*

Fermat little theorem(1640) :

let p a prime nombre and a an integer such that $p \nmid a$, we have then:

$$a^{p-1} \equiv 1 mod\ p$$

The theorem has been also discovered by **Leibnitz**, but its first proof was given by **Euler** in 1736, then also by **Gauss** in his *Disquisitiones*.

Examples:

$$100 = 10^{3-1} \equiv 1\ mod\ 3$$

and

$$(-4)^{5-1} \equiv 1\ mod\ 5$$

The reciprocal of **Fermat** result is false in general:

$$a^n \equiv a\ mod\ n \quad \nRightarrow n\ is\ prime$$

in the case when n is also a premier called *Carmichael number* , du to the American mathematician **Carmichael** (1879-1919) , the least one is 561. It has been proven in 1994 that there are infinitely of them[19].

Questions

i) give some sufficient condition for deciding that n is a prime

ii)

iii)

iv)

2) *Arithmetic functions*:

In order to well characterize the sequence of primes, on se sert beaucoup des *fonction arithmétiques* , elles sont dites *arithmétique* car elles prend leur values in $\mathbb{Z}$(we see later that even in $\mathbb{Z} + i\mathbb{Z}$) , one of their important proprieties is that they are *multiplicative*.

Definition :

We say that an arithmetic application f is multiplicative if

$$f(m.n) = (n).f(m)\ , \qquad \forall\, n, m \ \in \mathbb{N} \ \text{ and } \ (n, m) = 1$$

We say that f est *complètement* multiplicative

$$f(m.n) = f(n).f(m)\ , \qquad \forall\, n, m \ \in \mathbb{N}$$

The multiplicative propriety of an arithmetic application heritated from $\mathbb{Z}$. We

---

[19] A conjecture made by Carmichael after he had discovred them in 1909.

have already seen deux telles fonctions : $\tau(n)$, $\sigma(n)$ and $\varphi(n)$ .On va voir d'autres qui vont être utiles par la suite :

Möbius function :

The function of **Möbius** (1832) , known to **Euler**, is defined as

$$\mu(n) = \begin{cases} 1 \; si \; n = 1 \\ (-1)^r \; si \; n \; est \; le \; produit \; de \; r \; premiers \; distingués \\ 0 \; sinon \end{cases}$$

Exemples :

$$\mu(10) = 1 \quad , \; \mu(n^2) = -1 \;, (30) = -1 \;, \mu(25) = 0$$

the function $\mu(n)$[20] en quelque sorte éliminatee numberss that contain des powers ofprimes. We have two interesting facts about $\mu(n)$ and divisors d of n the first :

Theorem :

On a pour un entier n

$$\sum_{d|n} \mu(d) = 0$$

the second is the ***Möbius** inversion formula* , trouvée indépendamment by **Liouville** and **Dedekind**(1857) qui dit que :

---

[20] **Euler** conjectured that $\sum_{n=1}^{+\infty} \frac{\mu(n)}{n} = 0$, proved von **Mangoldt** by in 18.

Theorem :

if

$$f(n) = \sum_{d|n} g(d)$$

then

$$g(n) = \sum_{d|n} f(d)\, \mu(n/d)$$

On a une relation entre $\varphi(n)$ et $\mu(n)$

Theorem

on a pour $n \geq 1$

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

the **Möbius** function μ is multiplicative , but it is not complétement multiplicative.

Mangolt function Λ:

the German mathematician von **Mangolt** défined this function in 18 as follows

$$\Lambda(n) = \begin{cases} logp \; si \; n = p^m \\ 0 \qquad sinon \end{cases}$$

Examples :

$\Lambda(p) = logp,$ $\Lambda(6) = 0,$ $\Lambda(8) = log2$

It does roughly the inverse of ***Möbius*** *function*, elle élimine les nombres n qui sont un produit de nombres premiers p_i différents. La fonction Λ n'est pas

multiplicative.
On a quelques relations qu'on va voir ensuite

Theorem

$$\Lambda(n) = -\sum_{d|n} \mu(d) logd$$

we are interested by the behavior of these functions arithmetic .Par example la function $\tau(n)$ is very irregular elle prend la valeur 2 (pour $n = p$) une infinité de fois, alors pour bien avoir une idée de leur croissance on étudie la rapport

$$\lim_{n\longrightarrow\infty} \frac{\sum \ f(n)}{n}$$

On a quelques intéressing résults

Théorèm

$$\lim_{n\longrightarrow\infty} \frac{\tau(n)}{logn} = 1$$

$$\lim_{x\longrightarrow\infty} \frac{\sum_{n\leq x} \mu(n)}{x} = 0$$

$$\lim_{x\longrightarrow\infty} \frac{\sum_{n\leq x} \Lambda(n)}{x} = 1$$

by considering his function $\varphi(n)$, **Euler** generalized **Fermat** little theorem for arbitrary n :

Euler theorem(1740) :

Soit p un nombre premier et a un entier tel que $p \nmid a$ alors on a

$$a^{\varphi(n)} \equiv 1 \bmod n$$

with $\varphi(p) = p - 1$.

6):

There are some formulas that use the function $\pi(x)$.

Legendre(1808) des travaux sur $\pi(x)$ il trouva la formula

$$\pi(x) = \pi(\sqrt{x}) - 1 + \sum_d \mu(d)[\frac{x}{d}]$$

Des premiers distingués, il est plus facile d'étudier le problème par la fonction de **Möbius**

Primes in arithmetic progressions:

L'un des remarquables propreties of prime numbers est qu'on peut les classifier en categories de premiers à l'aide d'un linear polynomial (monôme) simple de la form

$$ak + b$$

tels que $(a, b) = 1$. Comme un exemple pour $a = 5$, b peut prendre les valeurs 1, 2, 3, 4 ce qui donne que la suite des nombres premiers est sur trois suites

i) $5\mathrm{k} + 1$: 11, 31,41,61, …
ii) $5\mathrm{k} + 2$: 2, 7,37,47, …
iii) $5\mathrm{k} + 3$: 13, 23, 43, 73,…
iv) $5\mathrm{k} + 4$: 19, 59, 79,89….

we have also a famous result du to **Dirichlet**

Theorem of **Dirichlet**(1837) :

Let a, b two entiers quelconques such that $(a, b) = 1$, then there exists infinity of nombres premiers dans la progression $an + b$.

The proof of this theorem uses also analytic methods qui nous allons voir dans la 3^{eme} partie. Cependant, on peut démontrer certain cas par des elementairy methods.

Example:

there exist an infinity of primes in the sequence: $4k + 3$.

Proof:
It is like the proof given by Euclid, supposons qu'il existe finite number de premiers dans la suite $4k - 1$ on leur produit

$$l = 4\prod_{k=1}^{n}(4k - 1) \ - 1$$

no one of the primes $4k - 1$ divdes the number l , suppose now that the set of the primes of the form $4k - 1$ is finite then ,

■.

Progression prims with prime ,in 2007 the following progression discovered that

$$56211383760397 + 44546738095860n$$

All primes for $n = 0, 2, \dots, 22$.

A conjecture called the *Baudet conjecture*, says that we divide ℕ by a law in any two sets we always find arithmetic progression of arbitrary length, it was proved by van der **Waerden**$(1903-1996)$ in 1927[21].

Form prime it is more difficult, In 2006, English Ben **Green**(born in 1977) and Chinese Terence **Tao**(born in 1975) proved this theorem

***Green-Tao** theorem* :

Let n a given integer, then there exists always a progression of length n all are primes.

It has been untill now , a dream to find a formula that gives all the rpeimes or at least only primes , this formula are invraisemblable du to the irregularity of la distribution des nombres premiers. La recherche a été initiated par **Euler** qui donna le polynomial

$$x^2 + x + 41$$

generating primes for $x = 0, \dots ,40$. We can give some more polynomials with rational coefficients, giving large sequences of primes for consecutive integers by using linear algebra, but the operation is not very practical.

It is very difficult to decide if a sequnece of number contains infinitly many primes , for example it is not known if the sequene

$$\begin{cases} u_n = u_{n-1} + 2n \\ a_0 = 11 \end{cases}$$

contains infinitly many primes. But the negative assertions are simpler to prove, **Goldbach** émet un intéressant résult

---

[21] See **Khinchin**.

Goldbach theorem (1752) :

There exists no polynomial of degree $n = 3$ that gives only prime numbers.

Euler has given a proof for every n (1762). It is easy to prove that the polynomial

$$ax^2 + bx + c$$

Cannot give primes only if $(a, b, c) = 1$.

We see that if the number of variables is greater than 1, then we have more chance to encounter primes .this is true for example for special polynomials of two variables called *quadratic forms* we will see in algebraic number theory. But in general it is very difficult to prove there exist infinitely prime in no linear polynomials.

Primality tests :

It is difficult to show that an integer n is prime, mathematicians have for long looked for methods to prove that a given integer is a prime:

On the prime factors of an integer we have a simple and practical result to test for primality:

Lemma:

Let $n = p_1 \times \ldots \times p_n$ an integer then we have to stop at max:

$$max(p_1, \ldots, p_n) \leq \sqrt{n}$$

The English **Waring** (1-1) , a student of **Wilson** enounced the following criteria in 1770 *:*

Wilson's theorem :

let n be an integer, then:

$$n|(n-1)\,!+1 \Leftrightarrow \quad (n\ is\ prime)$$

Il fut démontré par **Lagrange** en 1771. It is not practical at all.

the French mathematician **Lucas** (18-19) has given algorithm.

*Theorem (**Luca** 1891)* :

let an integer a such that : $a^{n-1} \equiv 1(\text{mod n})$ and $a^{(n-1)/p} \not\equiv 1(\text{mod n})$ pour tous $p|n-1$, alors n est premier.

tis result has been ameliorated since.

Other if some special numbers are primes or not : American mathematician Frank **Cole**$(1861-1926)$ needed 20 years in 1903 to find the factorization

$$2^{67}-1 = 193707721 \times 761838257287$$

In 1947, the American mathematician William **Mills**$(1921-1964)$ established that there exists a real number x_0 such that $[{x_0}^{3^n}]$ is always prime, this result has been ameliorated, see[].

Find algorithms that test if an integer n is prime which we call *primality test*. With the electronic revolution powerful computers and more powerful methods have been implemented. Before that mathematician had to the primes tables (factor tables also) the are those of Derrick N. **Lehmer**(1867-1938) in 1913 the last, however computers algorithm have made them obsolete.

Prime tests are also for time, the 2004 three scientist India that prime in polynomial time

Find Twin primes:

Another problem prime numbers, is the famous twins conjecture which is also an ancient problem[22] that asks If there exist infinitely many primes $(p, p+2)$.
The sieve method would be developed by Norwegian mathematician Vigo **Brun** $(1885 - 1978)$ in his article of 1920 , where he established that the series des inverses twin primes converges:

Theorem:
Pour $p \geq 3$

$$\sum_{p}\left(\frac{1}{p_n} + \frac{1}{p_{n+1}}\right) < +\infty$$

The sum $\sum_p\left(\frac{1}{p_n} + \frac{1}{p_{n+1}}\right)$ is named ***Brun constant*** , and is noted C_B.
We have an interessting proprety of these tewins due to American mathematician Paul **Clement**[23] in 1947 which is similar to **Wilson's** theorem :

Proposition :

the integer numbers n and $n+2$ are twin primes iff:

$$n(n+2) \mid 4(n-1)! + 4 + n$$

---

[22] See an article of **Dunham** in () origin of the twin conjecture.
[23] From the University of California.

see [ ] for a proof.

Exercises

1) in the second **Euclid** theorem prove that : $p_e > p_l$

1) give another reason it is not convenient to consider 1 a prime.

1) is every consecutive odd numbers always coprime?

1) let $n = p_1 \times \dots \times p_k$, show that : $\sqrt[k]{n} \leq \max(p_1, \dots, p_k)$

1) show that to test if n is prime , at least one of the prime factors cannot $< \sqrt{n}$.

1) Give an integer n such that one of its divisors $p > \sqrt{n}$. is it prime?

1) show that no odd integer of the form $4n - 1$ can a prime of the form $x^2 + y^2$.

1) what is the symbol $\left(\frac{a}{q}\right)$ in the case $p|a$?

1) calculate : μ (16), μ (200)

1) why is μ not completely multiplicative?

1) show that $\mu(p) = -1$ and $\sum_{d|p} \mu(p) = 0$

1) calculate : $\Lambda(16)$, $\Lambda(200)$

1) show that if f est multiplicative alors $f(1) = 1$, on déduire que Λ n'est pas multiplicative.

1) show that : $f(n) = n^r$ est multiplicative, isit completly multiplicative ?

1) let $n = {p_1}^{a_1} \dots {p_k}^{a_k}$, we define **Liouville** function

$$\lambda(n) = (-1)^{a_1 + \dots + a_k}$$

show that λ est multiplicative.

1) show that if: $(n,m) = 1$ then $\tau(nm) = \tau(n)\tau(m)$ and $\sigma(nm) = \sigma(n)\,\sigma(m)$. What about the case when $(n,m) \neq 1$?

1) write the number $2^{21} - 1$ comme une sum de puissance de 2

1) let $p \nmid a$, show that if : $a^p \equiv a \, mod \, p$ then $a^{p-1} \equiv 1 mod \, p$

1) write **Fermat** little theorem if $p|a$**.**

1) from **Euler** generalization, find **Fermat** little theorem.

1) show that the reciproque of **Fermat**'s little theorem is not necessarily true

1) soit p_{nj} the sequence of non-twins primes, show that : $\sum \frac{1}{p_{nj}} = +\infty$

1) soit p_i the sequence of primes, show that : $\sum \frac{p_i}{p_{i+1}} = +\infty$

1) soit p_i the sequence of primes, show that : $\sum \frac{p_{i+1}}{p_i} = +\infty$

1) by two methods, show that a progression $2n + 1$ contains infinitely many primes, $n \in \mathbb{N}$

1) show that existe une infinité de premiers de la forme $17n + 51$? why ?

1) conider the numbers: $3 \times 5 \times \ldots \times p_n + 1$, the product of n first primes except 2 . these number are even. Study the factors of these numbers.

1) we define : $p! = 2 \times 3 \times 5 \times 7 \ldots \times p$ (the primordial $p^{\#}$). Show that $p! + 1$ cannot be a square. What bout $p! - 1$?

1) show that $n! - 1$ cannot be a square.

1) use **Wilson** theorem to show that $n|(n-2)\,! - 1 \Leftrightarrow n$ is prime.

1) let $(p_j \, , p_{j+2})$ the twins: show that the series $\sum_{k=1}^{\infty} \frac{1}{p_{j+2} \times p_j}$ converges.

1) show that the series : $\sum_{k=1}^{\infty} \frac{1}{p_j} - \frac{1}{p_{j+2}} = 2 \sum_{k=1}^{\infty} \frac{1}{p_{j+2} \times p_j}$

1) Fermat affirmed he could prove that 2^{2^n} +1 is prime for every n. Give by computing a counter-example.

1) Imagine a mehod to know the number of digits of the number $2^{2020199}$

1) show that : $\varphi(p) = p - 1$, (**Fermat** little theorem is a particulier case)

1) why is φ not completely multiplicative?

1) Is 3 a primitive root of 7 ?

1) could you find a quadratic polynomial who gives the primes 11, 23, 47 for $n = 1,2,3$?(use matrices). Try third polynomial with the primes 29, 31, 71,73 for $n = 1,2,3,4$

1) show that the polynomial $x^3 + x^2 - 2$ cannot gives infinitly many primes

1) is there always primes between $n! + n$ and $(n+1)!$

1) infinitely many primes of the form $n_1! + 1$ and $n_2! - 1$.

Supplementary

1) let p_j and p_{j+1} two consecutive twin primes , show that , $12|p_j+p_{j+1}$

1) show that:

$i)$ $\left(\frac{pa}{q}\right)$ = $\left(\frac{p}{q}\right)\left(\frac{a}{q}\right)$

$ii)$ $\left(\frac{p}{qa}\right)$ = $\left(\frac{p}{q}\right)\left(\frac{p}{a}\right)$

1) Knowing that $\pi(x) \sim \frac{x}{logx}$ is a theorem, could you prove **Bertrand**'s conjecture?

Chapter 4

Distribution of Primes

One may ask: what make an integer n a prime? I have discovered an interesting trick to characterize a prime abstractly:

If we think in term of sets: consider n as the cardinal of a set E , the number of subsets of E is 2^n and when we eliminate E , ∅ and the singletons, the number of subsets becomes

$$A = 2^n - n - 2$$

than

Definition:

An integer n is a prime if we cannot classify n objects into sets E_i of a same cardinal such that we have for $k \neq l$

$$E_k \cap E_l = \emptyset$$

There is a curious relation between n and this number A : if n is prime it divides $2^n - n - 2$ (***Fermat's*** *little theorem*).

The distribution of primes has preoccupied mathematicians much since long, the sequence of primes p_i apparemmely does not follow law. We can find a long of no primes, we can find a lot of primes only by 2(the twin primes). **Euler** has declared :

« Mathematicians have sought an order in the sequence of prime numbers but it is a mystery that we cannot never penetrate »

For example it has been questioned, knowing p_n , can we know the value of p_{n+1} ? or more precesily knowing : $p_1 , \dots , p_n$, can we have information on the size of p_{n+1} ? we have some results:

Theorem:

$$p_{n+1} < {p_n}^n + 1$$

and

$$p_n < 2^{2^n} + 1$$

We will see that this question will be more treated the analytic number theory by examining the function $\pi(x)$ de more closely...
In 1845 French **Bertrand**(1-18) emitted the conjecture

There is at least a prime between n *and* $2n$

conjecture proved by **Tchebychev** in 1852. And in his he also another the following

It sis natural to ask how many primes are they between 2 and a given n. let this number by $\pi(n)$ then how is $[2, n]$ or better in $[2, x]$? Both **Legendre** and **Gauss** conjectured that $\pi(n)$ is very near to

$$\frac{n}{log(n)}$$

The century efforts led to an interesting result:

Hadamard-Lavallé-Poussin Theorem (1898) :

if the function π is defined as above , then as $x \to +\infty$

$$\pi(x) \sim \frac{x}{logx}$$

this is known as the *prime number thorem*, the proof of this theorem uses difficult analytic methods, It also gives the estimate

$$p_n \sim nlogn$$

the first proof elementary was discovered by Paul **Erdos**(19-19) and Atle **Selberg**(19-20) in 1947.

Since composite numbers are denser than prime ones, it is easier to prove result about them, like ***Simprinsky*** *number*,

in 196 **Simprinski** proved

Theorem

There is k odd the infinitely many k such

$$k2^n + 1$$

composite numbers for all n.

to generate primes it is very , if we define : $p! = 2 \times 3 \times 5 \times 7 \ldots \times p$[24] , how are the prime factors of $p! + 1$ and $p! - 1$?

---

[24] Noted also $p^{\#}$.

p	$p!-1$	$p!+1$
2	1	3
3	7	5
5	29	31
7	209	211
11	2309	2311
13	30029	30031
17	510509	510511

Distribution also twin numbers, the attempt were not very successful, but in 2013, the Chinese Yitang **Zhang** (born in 1955) proved a spectacular result:

Theorem

There are infinitely many primes p_i and p_j such that

$$p_i - p_j \leq 7 \times 10^7$$

The result has been afterwards is ameliorated by James **Maynard** (born in 1980) and others who could reduce the difference to 600.

The search caused the emergence of the function gaps between primes

$$g_n(x) =$$

Exercises

1) Show that there are infinitely many consecutive composite numbers of arbitrary length (think of $n!$).

Chapter 4

Diophantine equations

One of the preoccupations of Fermat was, following **Diophantus**, the search for *integer* solutions of polynomials equations. Today this sort of researches is known under the name of ***Diophantine*** *Analysis*.

A **Diophantine** equation is a polynomial equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

where we search for *national* or *integers* solutions.

Congruent numbers

A simple equation known to **Pythagoras** for a right triangle

$$x^2 + y^2 = z^2$$

which we know that it has infinity many solutions, if we interested of the area of this right triangle the following

Question

Are there triangles whose areas is a natural number n?

if this n exists then it is named *congruent number* . Of course such numbers exit, for example the number 6 is a congruent number as it is the area of the triangle (3,4,5) .

We can generalize this to a rational number x, y and z.

Bézout equality

we consider

$$ax \equiv d \mod n$$

that is equivalent to the Diophantine equation

$$ax + ny = d$$

before **Fermat**, **Bachet** influenced by the book of **Diophante**, studied a simple **Diophantine** equation called *linear* , he wrote his book *Pleasant problems*(1612) and give a problem like this :

Suppose one has 10 dollars and wants to buy pencils of 3 cents and pen of 5 cents, how many pen and pencils can he buy with 100 dolars?

this give the eqution[25]

---

[25] Such equations are called *indeterminate* because the problem posed is supposed to have a unique solution to determinate. The above problem has three solutions: (2,30), (8,20) and (14,10).

$$5x + 3y = 100$$

Then his result

Bachet theorem(1612, 1624):

Let a, b, x and $y \in \mathbb{Z}$

$$ax + by = 1 \quad ssi\ (a, b) = 1$$

This theorem is often attributed mistakly to **Gauss** and **Bézout** (also known under the anme of *inequality of **Bézout**)*, which may be reformulated

Theorem of **Bézout**:

Let $a, b \in \mathbb{Z}$ and $c = gcd(a, b)$ then there existe x , y such that

$$ax + by = c$$

this proved by **Bezout** for polynomials. we can more by dividing by d

$$ax' + by' = 1$$

get an equivalence

$$a \text{ and } b \text{ are coprime} \quad \Leftrightarrow \quad \exists x', y' : \ ax' + by' = 1$$

this means that if a and b are coprime so are x and y. **Bachet** theorem enters in the domain of simple *linear **Diophantine** equations* of the general form

$$ax + by = c$$

if a and $b \neq 1$, it is not certain exists solutions for on we do not know if $a|c - by$ or $b|c - ax$, we have a proved result

Theorem :

the Diophantine equation

$$ax + by = c$$

has a solution (x, y) iff $c|pgdc(a, b)$.

Example :

the equation

$$111x + 22y = 2$$

has no solutions because $2 \nmid 11$. But every one of the tw equations

$$12x + 6y = 3 \quad \text{and} \quad 24x + 16y = 2$$

has a solution because $3|3$ and $2|8$ respectively.

The solutions of an equation $ax + by = c$, the couples (x_i, y_i) , constitue in the plan $\mathbb{R}^2$ $une\ lattice$.

We can generilize the search for more than one variable which is more interesting. On va voir que lorsque l'équation est non linéaire la situation est plus difficile. Mais plus il y a de variables plus il y a de solutions.

Lagrange proved

Lagrange theorem :

let the polynomial

$$p_n(x) = a_n x^n + \cdots + a_1 x + a_0$$

and p a prime such that : $p \nmid a_n$ alors $p | \, p_n(x)$ pour au plus n valeurs de x.

Pell equation

It is classical problem to find integer solutions to the equation

$$x^2 + y^2 \ = a$$

we can simplify it if $a = bc$: $z^2 + t^2 \ = b$ and $l^2 + m^2 \ = c$ because

$$(z^2 + t^2)(l^2 + m^2) = (zl - tm)^2 + (zm + lt)^2 \quad = x^2 + y^2$$

It is not known why Fermat studied the Diophantian equation

$$x^2 - ay^2 \ = 1$$

with a is not a scquare. **Euler** has made an error by attributing it to John **Pell**[26] (1611-1685)(friend of **Waring**) who was interested in number theory. The equation is now known under the name of *Pell equation*. This equation will be important in the theory of quadratic forms in two variables x and y.

We have a classical result :

Lagrange theorem:

---

[26] He is known for publishing a list of 100000 primes in 1668, and a list of 10000 squares in 1672.

The equation $x^2 - ay^2 = 1$ has infinitely many integer solutions .

On va voir que l'équation de Pell va être traitée par d'autres méthodes algébriques. Une conjecture dans ce domaine due au mathématicien français Eugène **Catalan** (1814-1894) en 1844 dit que Diophantine equation

$$x^{k_1} - y^{k_2} = 1$$

Has for solutions only $y = k_1 = 2$ et $x = k_2 = 3$, elle n'a été démontrée qu'en 2004 par le mathematician roumain **Mihăilescu** (born in 1955).
Une ***Diophantine*** *equation* particularly important est equation de la form

$$y^2 = ax^3 + bx^2 + cx + d$$

that is plan *elliptic curve*, elle sera important dans la partie algébrique et analytique , ces courbes sont la clé pour la solution du GTF par **Wiles** et **Taylor** en 1994-1995. Another famous conjecture related to these ellipti is the Birch-Swinnerto-Deyer conjecture.

Hilbert tenth problem

Diophantine analysis has seen more advanced developments when in 1900 **Hilbert** asked the mathematical community to find an algorithm that i precise if a given Diophantine equation has solutions, we have since then some results :

Theorem of Siegel (19) :

A cubic equation has at most a finite number of integer solutions.

The problem has been solved in 1970 by Russian **Matiyasevich** (1947-) : there does not exist an algorithm that decide if a given Diophantine equation has solutions. This domain was enriched afterwards in the years 1980's by the ABC conjecture or the **Oesterlé**-**Masser** conjecture:

The ABC Conjecture

let a, b, et c three coprime integers with $c = a + b$, then

$$c > rad(abc)^{1+\varepsilon}$$

the ABC conjecture implies a lot of not yet proved results in number theory.

Exercises

1) Indicate the congruent numbers from

5, 7, 8, 9, 10, 11

1) Show if a is a congruent number, then ab^2 is a congruent number too.
1) find the solution of

$12x + 6y = 3$, $24x + 16y = 2$, $21x + 14y = 7$

1) show that if $(a, b) = 1$ alors $\exists\ x$ et $y \in \mathbb{Z}$ tels que $ax + by = 1$ (Bézout⇒ Bachet)
1) for which integers k and y is $\sqrt{-4y^2 + 4k - 3}$ an integer ?
1) find solutions de **Diophantine** equation $4x^2 - y^2 + 4x + 1 = 0$
1) what condition on integers x and y such that $\frac{xy+1}{x+y}$ is always an integer ?
1) show that: $2x + y = 1$ a une infinity of integer solutions.

1) trouver integer solutions de $x + 6y - 6z = 1$, existe-il une infinité ?

1) show that for every natural n , $x^2y^2 + xy + 1 - n + x^2 = 0$ has infinity many integer solutions

1) montrer que Diophantine equation $4x + 6y = 11$ n'a pas de solution

1) the solutions of $x^2 - y^2 = 1$ (Pell equation for $a = 1$).

1) suppose that a Diophantine equation a rational solution, has it also an integer solution?

1) let the linear equation

$$a_1x_1 + \cdots + a_kx_k = n$$

where $a_1, \dots, a_1, n$ are integers. Discuss the exitence of integer solution and their numbers.

1) solve the equation : $k^4 + k^2 = n^2 + n$ in integers.

Chapter 5

Theory of partitions

The first to partitions was **Euler** he how amny can we write an integer as a sum of smaller intgers, he thus creted the *generating series*, the forunner of other theorie seen in analytic number theory. We here ex problems that has some relation with quadratic forms.

Sum of powers :

One of the classiques problèmes intrested in XVIII century,est de pouvoir écrire un entier n comme la somme des puissances d'entiers r_i

$$n = \sum_i {r_i}^k = {r_1}^k + \cdots + {r_l}^k$$

Dans ses Fermat avança que

-tout entier triangulaire est la somme de 2 ou 3 nombres triangulaires

-tout entier n est un carrée ou la somme de 2, 3 ou 4 carré

-tout entier est un nombre pentagone ou la somme de 2,3,4 ou 5 nombres pentagones

Fermat s'inspirant des de l'*Arethmetica* de Diophante et peut-être lui-même inspiré des triplets de Pythagore $a^2 + b^2 = c^2$, s'intéressera d'écrire les

entiers comme la somme de 2 carrées

$$n = x^2 + y^2$$

ce qui l'amené à conjecturé (et avant lui Girard en 16) que tout nombre premier p de la forme $p = 4k + 1$ peut être décomposé en deux carrée sans donner une démonstration, Euler donna une démonstration en 1747.

Fermat aussi conjectura que tout entier n est la somme de 4 carrées. En 1770 Lagrange prouva

Lagrange Theorem:

Every naturel integer n is the sum of 4 square numbers, of which some are null.

Example :

$1 = 1^2 + 0^2 + 0^2 + 0^2$
$2 = 1^2 + 1^2 + 0^2 + 0^2$
$3 = 1^2 + 1^2 + 1^2 + 0^2$
$4 = 1^2 + 1^2 + 1^2 + 1^2 = 2^2 + 0^2 + 0^2 + 0^2$

Lagrange theorem leads us to introduce the definition of an interesting concept last chapter:

Definition :

On dit qu'une suite u_n est une *base of order* k si la somme de k fois de la suite u_n nous donne tout l'ensemble des entiers $\mathbb{N}$.

Lagrange theorem tells us that the sequence of squares is a basis of order 4 ,car la combinaison de 4 de ces squares nous give all the positive integers. Dans d'autres cas on s'intéresse pas à tous les entiers, mais à tous les entiers assez grand,

Waring problem

in 1792 **Waring** émet an interesting conjecture : let n any integer number , we can write n as the sum of 4 squares, 9 cubes, 19 d'entiers du 14th power …

Hilbert montra qu'une généralisation du résultat de Lagrange.

Hilbert theorem (1909) :

On $\forall\, n, \exists k, \exists l$

$$n = {r_1}^k + \cdots + {r_l}^k$$

Ces spéculations nous amènent à définir le nombre $g(k)$

Definition :

On dit $g(k)$ est le plus petit entier k vérifiant

$$n = {r_1}^k + \cdots + {r_{g(k)}}^k$$

On a quelque exemples connus :

$$g(3) = 9\,,\ \ g(4) = 19\ \ , g(5) = 37\ \ \ ,\ \ g(6) = 73$$

Dans son problème de trouver puis **Hardy** et **Littlewood** qu'une borne pour k. ces questions vont être étudiées dans la théorie additive des nombres.

Additive partitions :

Dans la même philosophie on ne cherche pas la somme des puissances mais la somme : De combien de façons on peut écrire un number n comme somme de nombres entiers ? Ce problem est appelé *problem de partitions*, par example le number 5 peut être partitionné de 7 façons

$$\begin{aligned}5 &= 1+1+1+1+1 = 1+4 = 2+3 = 2+2+1\\ &= 2+1+1+1\end{aligned}$$

Le problème a été étudié par Hardy et l'indien Ramanujan (1887-1920) qui ont montré

Theorem :

le nombre des partitions d'un nombre entier n noté $p(n)$ est estimée à

$$p(n) \sim \frac{e^{c\sqrt{n}}}{4n\sqrt{3}}$$

Ou le symbole $\sim$ veut dire

$$\lim_{n \longrightarrow +\infty} \frac{p(n)}{\frac{e^{c\sqrt{n}}}{4n\sqrt{3}}} = 1$$

avec $c = \pi\,(\frac{2}{3})^{1/2}$.

Tous ces résultats sont plutôt étudiés dans la théorie additive des nombres dans la partie analytique.

Goldbach's even and odd conjectures

in the same related problem, we search for more interesting partitions but more difficult. In a letter to **Euler** in 1742 , **Goldbach** conjectured that

Every even integer n may be as the sum of two primes

It has also been conjectured that

Every odd integer $n \geq 7$ *may be the somde three prime numbers*

The last conjecture is implied by that of **Goldbach**. In 1937, Soviet matheamtician **Vinogradov** $(1891 - 1983)$ proved the weak **Goldbach** conjecture:

Vinogradov theorem:

there exist a number n_V ssuch thata for all positive integrs $n > n_V$, n est la somme de 3 nombres premiers.

Vinogradov has shown that a the sequence of premier number s est une base d'ordre 3 for $\mathbb{N}$. La preuve utilise des méthodes analytiques. the number n_V is huge and is estimated in 2002 à la borne

$$n_V < 10^{1346}$$

To complet the proof one must check all the numbers $< 10^{1346}$, a task that is not practical. But in 2013 , the Peruvian mathematician H. **Helfgott** (born in 197) has given a definitive proof for $n > 5$.

Exercises

1) Show that the even Goldbach conjecture implies the theorem of *Vinogradov*.
1) show that the theorem de **Vinogradov** implies that every even n est la somme de quatre premiers.
1) show that every integer n suffisamment grand peut être écrit comme somme de quatre premiers.
1) in the even conjecture of **Goldbach** study the number of to write an even number as the sum of two primes and for n 100 and give your conjecture

Chapter 5

Quadratic forms

This chapter is a subsequent of the previous one. The word *form* is due to **Euler** who used it in the XVIII century to designate a *polynomial*. This originated from **Diophontus** like $x^2 + y^2 = a$ when **Fermat** his $x^2 + y^2$ conjectures, general quadratic forms were introduced.

Binary quadratic forms

Naturally after linear forms $ax + by$, which are of degree 1, we find ourselves interested in the forms of degree 2 , they are the quadratic forms. after **Fermat** many conjecture about them especially the form

$$x^2 + 5y^2$$

Lagrange(17-18) studied them systemically. What interest us here is the binary quadratic forms, this form is a polynomial in two variables

$$q(x,y) = ax^2 + bxy + cy^2$$

Such that a, b and c are integers.
we have already seen early results conjectured by **Fermat** was that every prime of the form $4n + 1$ can be written

$$x^2 + y^2$$

This the case when $a = c = 1$ and $b = 0$. **Fermat** every prime number of the form $8n + 1$ peut written binary

$$x^2 + 2y^2$$

proof following **Euler's** . it has been shown that the even **Goldbach** conjecture is equivalent to

$$x^2 + y^2 = pq$$

To the number that a quadratic form may give, we a lot of negative more or always positive or especially primes. then we a as follows:
the form is *positive definite* if it only positive, and *definite negative* only negative , the $-2x^2$ is definite negative. it is *Semipositive* definite if it gives nul and positive numbers. If the form gives both positive and negative it is called *indefinite*.

In the case of binary quadratic form the

$$(x_1, x_2)\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

The determinant of A is $ac - b^2$ is the discriminant of the form.

We can the equivalence of two quadratic form by their matrices, we say that a matrix A is equivalent to matrix B if exist P, P such that

$$A = PBP^{-1}$$

we by AB.

Class number

Quadratic forms afterwards studied by **Lagrange** en 1773 , he defined its *discriminant* for a binary quadratic form

$$q(x, y) = ax^2 + bxy + cy^2$$

By

$$D = b^2 - 4ac$$

Observation

If $D_1 \neq D_2$ the two are not equivalent but if $D_1 = D_2$ then it may be or may be not equivalent.

we can easily give a form find another equivalent form by a linear transformation:

$$\begin{cases} x = \alpha z_1 + \beta z_2 \\ y = \gamma z_1 + \delta z_2 \end{cases}$$

The first thing is to equivalent forms they give the same number.

$$q_1(x, y) \sim q_2(x, y)$$

Example

let the form $q_1 = ax^2 + bxy + cy^2$ by th transformation

$$\begin{cases} x = z_1 + z_2 \\ y = z_1 + z_2 \end{cases}$$

we find a new equivalent form $q_1 = a{z_1}^2 + z_1 z_2 + z_2$.

As $q_1 = xAx^T$ and $q_2 = yBy^T$ then

$$A = SBS^T$$

Questions

i) Give sufficient condition to q_1 and q_2 to be equivalent

ii) What is the nature of the numbers given by a binary form q ?

iii) what relation between D and these numbers?

iv) are there infinitely many primes in q ?

Lagrange e tried to classify according to the number D. He discovered the *class number* **. Lagrange** found that for a give D there it is a *number class* , a natural number noted h_K (we will later know why).

Definition

The class number is the number of distinct forms with the same determinant D (positive or negative).

Or the same, it is the number nonequivalent forms with a given determent D. the problem there exist nonequivalent forms with the same determinant.

Lagrange proved

Theorem:

There exists a finite number of *classes* of quadratic forms for a given D

Puis chercha un procédé de transformer une forme quadratique q à une forme q'.

Theorem:

Let a form then we can change by linear to the

$$\sum_{ij}^{n} a_{ij}x_i x_j$$

To

$$y + \cdots + y$$

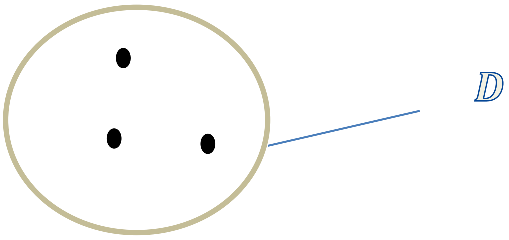


Fig for D= there three equivalent forms so $h_K = 3$.

Gauss

Gauss a lot quadratic forms in his book *Disquisitiones*, in 17 he wrote a binary quadratic form as

$$ax^2 + 2bxy + cy^2$$

and defined its *discriminant* D as

$$D = b^2 - 4ac$$

In manipulating quadratic forms, Gauss for the first time discovered the *group* structure. He calculated by hand the class number for thousands of determinants but he could not find the general formula for the class number.

Dirichlet

Neither Lagrange nor Gauss succeeded in giving a formula for the class number, a task that will be fulfilled by Dirichlet.

Theorem:

Let a form then we can change by linear to the

$$D(\quad) = \sum_{ij}^{n} a_{ij} x_i x_j$$

Other discussions et developments will be seen in the part of algebraic number theory .

The first paper of **Dirichlet**(1833-35) on the primes in a quadratic form. He used reciprocity law to settle the problem

Dirichlet proved the following theorem

Theorem (18)

let $ax^2 + 2bxy + cy^2$ be a quadratic form with $(a, 2b, c\ ) = 1$ there exists an infinity of primes.

The complete proof has been given by German mathematician **Weber**(18-1) in 18.

General quadratic forms

If the 3 the ternary form.

Definition

a general quadratic form is of the form

$$f(x_1, \dots, x_n) = \sum_{ij}^{n} a_{ij} x_i x_j$$

where all the terms x ont le same degree 1.

as examples:

$$7x^2 \quad , \quad {x_1}^2 - x_1 x_2 + 7{x_2}^2 \quad , \quad ax^2 + by^2 + cz^2$$

We are here interested in integer solutions and we know since Antiquity that infinitely solutions of the quadratic form

$$x_1 x_1 + x_2 x_2 - x_3 x_3 = 0$$

which is simply the Phythagorian theorem. Le domaine est très vaste avec des aspects élémentaire, algébrique et analytique. On peut aussi les traiter par les methods of linear algebra : on peut écrire une forme quadratique as a product vector-matrix-vector

$$\sum_{ij}^{n} a_{ij} x_i x_j = (x_1, \dots, x_n) \begin{pmatrix} a_{11} \dots & a_{1n} \\ \vdots & \vdots \\ a_{n1} \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix}$$

where $\begin{pmatrix} a_{11} \dots & a_{1n} \\ \vdots & \vdots \\ a_{n1} \dots & a_{nn} \end{pmatrix}$ is a suitable squared matrix :in fact *lemma*:

the matrix A for a quadratic form is *symmetric*.

the quadratic form can be written as

$$q = xAx^T$$

For a linear form the matrix is a line vector.

Exercises

1) write the matrix for a linear form .

1)show that in a binary quadratic form $q = xAx^T$, it is simpler to consider A as symmetric

1) is there a difference between the two quadratic forms: $x^2 + ay^2$ and $bx^2 + cxy + dy^2$?

1) indicate the definiteness of the following quadratic forms

a) $x^2{+}2y^2$

b) $t^2 - 3y^2$

c) $2z^2 + zy + y^2$

a) $x^2 - xy - 2y^2$

b) $t^2 + 3ty + 3y^2$

c) $2z^2 + zy - 2y^2$

1) write the following quadratic forms by matrix notation

a) $x^2 - xy + 2y^2$

b) $t^2 - 2ty + 3y^2$

c) $2z^2 - zy + y^2$

1) give equivalent quadratic forms to the following
a) $x^2 + xy + y^2$
b) $3t^2 - 2ty - 3y^2$
c) $2z^2 + zy + y^2$

And find A,B and S.

1) let the following quadratic forms
a) $5x^2 - xy + y^2$
b) $t^2 - 5ty + 3y^2$
c) $z^2 - zy + 3y^2$
détermine le D according to **Lagrange**

1) let the following quadratic forms
a) $x^2 - 2xy + y^2$
b) $t^2 - 5ty + 4y^2$
c) $2z^2 - zy + y^2$
déterminer le D according to **Direchlet**

1) let the following quadratic forms
a) $x^2 - xy + y^2$
b) $3t^2 + ty + 2y^2$
c) $z^2 - zy - 2y^2$
determine D according to **Gauss**.

Chapter 8

Bernoulli Numbers

Opolka p. 28.

We have consider the triangular numbers

$$\sum_{k=1}^{k=n} k^1 = 1 + 2 + 3 + \ldots + n = \frac{1}{2}n(n+1)$$

We try now considering the general sum $\sum_{k=1}^{k=n} k^r$, $r = 2,3, \ldots$:

$$\sum_{k=1}^{k=n} k^2 = 1 + 2^2 + 3^2 + \ldots + n^2 = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$

compactly

$$\sum_{k=1}^{k=n} k^3 = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2 + 0n$$

$$\sum_{k=1}^{k=n} k^4 = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 + 0n - \frac{1}{30}n$$

$$\sum_{k=1}^{k=n} k^5 = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 + 0n - \frac{1}{30}n$$

$$\sum_{k=1}^{k=n} k^6 = \frac{1}{4}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2$$

$$\sum_{k=1}^{k=n} k^7 = \frac{1}{4}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2$$

$\sum_{k=1}^{k=n} k^8 = \frac{1}{4}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2$

…… so on.

It is why 0 some terms and numbers keep appearing always some

$$\frac{-1}{2}, \quad \frac{1}{6}, \quad \frac{-1}{30}$$

ou dans le cas général on voit toujours apparaitre les nombres notés B_n

$$\sum_{n=1}^{n=k} k^r = \sum_{k=0}^{k=n} \frac{B_n \,.\, k\,!}{k\,! + k - 1\,!} n^{k+1}$$

Constant numbers

These are always numbers that do not change , they are

$$B_0 = 1 \quad , \quad B_1 = \frac{-1}{2}$$
$$B_2 = \frac{1}{6} \quad , \quad B_3 = 0$$
$$B_4 = \frac{-1}{30} \quad , \quad B_5 = 0 \ldots$$

and !

$$B_{34} = \frac{2577687858367}{6}$$

These rational nymbers B_n are called *Bernoulli Numbers* , il sont apparu pour for the first time in the book 1713 in *Ars Conjectandi* (1713), a posthumus work on probability written by Jacques **Bernoulli**. Ils sont appelés ainsi par à **Moivre**.

the odd numbers B_n (when n is odd) are all nul for $n > 1$. On a

$$B_n \;=\; \sum_{k=0}^{n} \binom{n}{k} B_k$$

They are very obscurs numbers que nous trouverons dans plusieurs series. Ils apparient dans bien other formulas. Ils sont les coefficients in the infinite series of the function

$$\frac{x}{e^x - 1} \;=\; \sum_{n=0}^{n=\infty} \frac{B_n x^n}{n\,!}$$

Euler (17). On a aussi la formule noté aussi

$$\sum_{n=1}^{n=k} \frac{1}{k^r} \;=\; \sum_{n=0}^{n=\infty} \frac{2^n |B_n|\, \pi^n}{2(k\,!)}$$

Une relation avec les nombre premier de n

von **Staut-Clausen** (1840) :

Let B_n the Bernoulli numbers , then

$$\sum_{n=1}^{n=k} \frac{1}{p} + B_n \in \mathbb{Z}$$

Ces nombres trouveront une importante utilisation dans la théorie des nombres en général et aussi dans la solution du Grand Théorème de Fermat. On va les rencontré beaucoup dans ce livre. On a la formule d'Euler-Maclaurin

Euler-Maclaurin Formula

$$\sum_{n=1b}^{n=b} f(n) = \int_a^b f(x)dx + \frac{f(a)+f(b)}{2} + \sum_{n=a}^{n=b} \frac{B_n}{2}$$

Bernoulli polynomials

A côté des nombres de Bernoulli, on définit aussi les *polynomials of Bernoulli*. A Bernoulli polynomial $B_n(x)$ is définied as

$$\begin{cases} B_0 = 1 \\ \forall n, \int_0^1 B_n(x)dx = 0 \\ B_{n+1} = (n+1)B_n \end{cases}$$

Ils sont donnés aussi à m'aide des nombres de Bernoulli

$$B_n = B_n(0)$$

Et aussi

$$B_n(x) \quad = \quad \sum_{k=0}^{n} \binom{n}{k} B_n x^{n-k}$$

Aussi apr pour $n \geq 1$

$$B_n(x+1) - B_n(x) \quad = \quad nx^{n-1}$$

Ce qui donne

$$B_0(x) \quad = \quad 1$$

Il sont aussi impliqués dans le calcul de la fonction zeta de Riemann

Ils pour $|z| < 2\pi$

$$\frac{ze^{xz}}{e^z - 1} = \sum_{n=0}^{n=\infty} \frac{B_n(x)}{n\,!} z^n$$

Very curiously they jumped in **Kummer** work on FLT , as he looked for regular primes (see second part).

Binomial coefficients

Other numbers looks like strngely , appear like the de Bernoulli numbers, des coefficients dans un produit de n binômes

$$(a+b)^n$$

Ils ont été étudiés par les, puis Pascal et Newton

$$(a+b)^n = \binom{n}{0} a^n + \binom{n-1}{1} a^{n-1} b + \cdots + \binom{n}{n} b^n$$

Ou les coefficients $\binom{n}{k}$ sont des nombres entiers définis par la notation anglo-saxonne

$$\binom{n}{k} = \frac{n\,!}{k\,!\,(n-k)\,!}$$

Aussi la notation française moins pratique

$$C_n^k = \frac{n\,!}{k\,!\,(n-k)\,!}$$

Appreas in many like Leibnitz derivation

$$(f.g)^{(n)}(x) \;=\; \sum_{k=0}^{n} \binom{n}{k} f^{(n)}.g^{(n-k)}$$

Exercises

1) if you know that

$$\sum_{k=1}^{n} k^2 = \frac{n(2n-1)(2n+1)}{6}$$

find $\sum_{k=1}^{n}(2k-1)^2$.

1) find the sum

$$\sum_{k=1}^{k=n} k^4$$

1) let *triangular number* t_n, show that : $t_n = \binom{n+1}{2}$

2) utiliser la formula de **d'Euler**-**Maclaurin** somation pour approximer les sommes

$\sum_{r=0}^{n}(1/2)^n$, $\sum_{r=0}^{n}()^n$, $\sum_{n=1}^{10} 1/n$, $\sum_{r=0}^{n}(-1)^n$, $\sum_{r=0}^{n}(-1)^n$

1) soit $n, r \in \mathbb{N}$, show that : $\binom{n}{r} = \binom{n}{n-r}$

1) show that : $n^2 = \binom{2n}{2} - 2\binom{n}{2}$

1) show that : $2^n = \sum_{r=0}^{n}\binom{n}{r}$

1) show that : $\sum_{r=0}^{n}\binom{n}{r}(-1)^n = 0$

1) Explain why if you sum the digits of ten consecutive number you always the sequence 1,…,9.

1) let n a integer , show that : $n \left| \frac{n!}{k!(n-k)!} \right.$

Chapter 8

Transcendental numbers

In this theory, to which mathematicians has given the general name *transcendental number theory*, four subjects are studied:

$i)$ Irrationality.
$ii)$ algebraic and transcendental numbers.
$iii)$ linear independence.
$iv)$ algebraic independence.

I will give here only some notions on this difficult domain, for more information, the reader interested in the theory of transcendental numbers can consult [H][N][] for other developments, [B] is more difficult. We will see here some results since Euler and methods that can be used to show that a real number is irrational, and other methods can be used to show that a real number is transcendental.

Irrational numbers:

We say that a number r is *rational* (from Latin "$ratio$" which means ratio) if we can write r as a ratio of two integers $a, b \in \mathbb{Z}$

$$r = \frac{a}{b}$$

where the fraction $\frac{a}{b}$ is *irreducible* , which means that $(a, b) = 1$, we say also that $\frac{a}{b}$ is *in lowest terms*.

Example :

$$0,4 = \frac{2}{5} \qquad , \qquad -1,012345679\ldots = \frac{-82}{81}$$

So a rational number is constituted of an entire part and of a decimal(fractional) part, the decimal part is either finite or infinite periodic, a period is a repeated pattern of numbers. Any integer $n \in \mathbb{Z}$ is a rational as $n = \frac{n}{1}$.

Usually to highlight the period, we put a line over the repeated decimal numbers

$$\frac{5}{7} = 0,\overline{\mathbf{714285}}714285\ldots$$

In a rational number, there may be an arbitrarily number of *chaotic* sequence of numbers before the number pattern stabilizes and become periodic

$$\frac{a}{b} = x, x_1 x_2 x_3 \ldots . \overline{\boldsymbol{abcdef}} abcdef \ldots$$

The set of rational number sis noted by the symbol $\mathbb{Q}$.

A *decimal* (from *decima* : ten)number is a rational number of finite decimal part, it is called decimal because it can be written it in the form

$$r = \frac{a}{10^n}$$

the denominator is a power of 10. And since the proper divisors of 10 are 2 and 5 and since a is arbitrary then r is usually written in the form

$$r = \frac{c}{2^t 5^s}$$

where the denominator has only powers of the numbers 2 and 5, the sole divisors of 10, we can show that these numbers have a finite decimal part and thus the period is 0 as in

$$\frac{7}{2} = 3{,}5\overline{\mathbf{0}}\ldots$$

An *__irrational__* number cannot be written in the form of a fraction $\frac{a}{b}$ where both a and b are integers. It is also called an *__incommensurable__* number, for the integer a and b have not a common measure unity 1, at the contrary of a rational number such as

$$\frac{3}{2} = \frac{1+1+1}{1+1}$$

the set of rational numbers is noted by $\mathbb{I}$.In fact $\mathbb{R}$ is composed of rationals and irrationals, there no other numbers so

$$\mathbb{R} = \mathbb{Q} \bigcup \mathbb{I}$$

And

$$\mathbb{I} = \mathbb{Q}^c$$

It is evident how to construct a rational number, but how can we construct irrational numbers? The first by :

Theorem :

The number x is rational $\Leftrightarrow$ x has a periodic fractional part.

Heuristically since every irrational is non-periodic , then we can construct irrational numbers by a non-periodic decimal part

$$\alpha = 1{,}0100100010000100000 1 \dots$$

In the decimal part, the number of "0" between the ‘1’ goes by augmenting indefinitely, and this cannot be periodic. So are numbers of the form

$$\sum_{n=0}^{\infty} \frac{1}{10^{n\,!}}$$

this cannot have a periodic decimal part, so it is irrational.

The main other way to do that is by the *surds* $\sqrt{n}$, where n is square free ($n \neq k^2$) so any number has a surd is irrational. One of the earliest results of the theory of irrationals numbers was the discovery of the irrationality of the surd number $\sqrt{2}$ in an event that spoiled the Greek theory of integers.

Theorem :

The number $\sqrt{2}$ is irrational.

Proof :

Let a and b two integers such that $(a, b) = 1$ and $\sqrt{2} = \frac{a}{b}$ then $2b^2 = a^2$, which gives : $2|a$ and consequently $2|b$ (as 2 is a prime) , a contradiction with $(a, b) = 1$■

We say that $\sqrt{2}$ is a *quadratic* irrational because it verifies a quadratic polynomial equation $x^2 - 2 = 0$. It is easy to show that the numbers $\sqrt{2(2n+1)}$ are irrational when $n \in \mathbb{N}$. The reader can prove that for every *square free* integer $n \in \mathbb{N}$

$$\sqrt{n}$$

is also irrational.

The set of rationals $\mathbb{Q}$ is *dense* in $\mathbb{R}$ in a sense that between any two irrational numbers α and β there a rational number r. In terms of general topology , we say that $\mathbb{R}$ is the closure of $\mathbb{Q}$ and $\mathbb{I}$

$$\mathbb{R} = \overline{\mathbb{Q}} = \overline{\mathbb{I}}$$

There is much more irrationals than rationals , so the set of rationals is denumerable

$$Card(\mathbb{Q}) = \aleph_0$$

But

$$Card(\mathbb{I}) = Card(\mathbb{R}) = \mathfrak{c}$$

Because of this density, a relation between rational numbers and irrationals which is very evident:

Lemma:

Every *irrational* number x can be approximated by a rational number in the wanted precision: $\forall\ x$ irrational , $\forall \epsilon > 0,\ \exists a$ and b with $b \neq 0$ such that

$$\left|x - \frac{a}{b}\right| \leq \epsilon$$

so any irrational number

$$\frac{a}{b} < x < \frac{a+1}{b}$$

in this way the magic irrational number $\pi = 3{,}14 \ldots$ can be approximated as :

$$3{,}14159264 \ldots < \pi < 3{,}14159266 \ldots$$

Another interesting idea saw the day and can be a means to characterize irrational numbers : what is the relation between ε and the numbers a, b ? otherwise, how is rapid this approximation ? we have an old result

Theorem

Let x be any irrational number, then there exits infinitely many rationals $\frac{a}{b}$ s.t :

$$\left|x - \frac{a}{b}\right| < \frac{1}{b^2} = \epsilon$$

This is called the ***Dirichlet*** *approximation theorem* proved by him in 1842. To prove it he used the pigeon.

We say that the number of solutions (a, b) for the equation $\left|x - \frac{a}{b}\right| < \frac{1}{b^2}$ is infinite.
In 1891, German mathematician Adolf **Hurwitz** $(1854 - 1919)$ proved the following result:

Hurwitz theorem

For any *irrational* number x there is infinitely many numbers $(a, b) = 1$:

$$\left|x-\frac{a}{b}\right|<\frac{1}{b^2\sqrt{5}}$$

this theorem shows also that $\sqrt{5}$ is the best, if we try another $>\sqrt{5}$ as , we find that the inequality

$$\left|x-\frac{a}{b}\right|<\frac{1}{b^2\sqrt{6}}\quad<\frac{1}{b^2\sqrt{5}}$$

has a *finite* number of solutions $\frac{a}{b}$.

Classical methods for irrationality:

As we know $\mathbb{Q}$ is denumerable $Card(\mathbb{Q})=\aleph_0$ rational numbers are very rare,

so we have

Heuristically:

If we pick a real number x from the real line we have

$$Probability(\,x\text{ is }\boldsymbol{rational})=0$$

We say also that the Lebesgue measure of $\mathbb{Q}$ is 0 : $\mu(\mathbb{Q})=0$.

So for every complicated formed number it is very likely that it is irrational. This is the case with the numbers $log(x)$ where x is rational. In his book *Introductio* (p.80), **Euler** has already remarked

Unless the number b *is a power of the base* a*, the logarithm of* b *cannot be expressesd as a rational number. If, indeed* $log(b) = \sqrt{n}$*, then* $a^{\sqrt{n}} = b$*, but this is impossible if both* a *and* b *are rational*[27]*.*

He means that if $log_a(b) \in \mathbb{Q}$, then b should $= a^r$, where $r \in \mathbb{Q}$ and a the base ($log(a) = 1$). In 1744, **Euler** proved the irrationality of e. The number e is defined as

$$e = \lim_{n \to +\infty} \left(1 + \frac{1}{n}\right)^n$$

It has the infinite series representation

$$e = \sum_{n=0}^{+\infty} \frac{1}{n!}$$

Proof:

We have $e = \sum_0^{k+1} \frac{1}{n!} + \sum_{k+} \frac{1}{n!}$.

The number π has the following series

$$\pi = 4 \sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1}$$

In 1766 the Suisse **Lambert** $(1728 - 1777)$ proved the irrationality of the number π, his proof was incomplete, and rectified by **Lagrange** later[28]. Quite recently! We are going to give a short proof of the irrationality of π due to American mathematician Ivan **Niven** $(1915 - 1999)$ found in 1947 :

Suppose that : $\pi = \frac{a}{b}$ with $(a, b) = 1$, and define the function f such that

---

[27] It is to note that mathematicians of the time mean by rational " algebraic", but this is not precise , as there are irrationals that are not algebraic.

[28] See **Struik** source in mathematic.

$$f(x) = \frac{x^n(a-bx)^n}{n\,!}$$

We see that $f(x) = f(\frac{a}{b} - x)$. We define another function in derivatives of f :

$$F(x) = \sum_{k=0}^{2n} (-1)^{2k} f^{2k}(x)$$

■

In 1748 **Euler** showed that the numbers

$$\zeta(2k) = \sum_{n\geq 1} \frac{1}{n^{2k}}$$

are irrational. Regarding the numbers $\zeta(2k+1)$ we have a unique result due to the French mathematician Roger **Apéry** $(1916 - 1994)$ who proved in 1978 that $\zeta(3)$ is irrational. However, in 2001 , it has been proved by French Tanguy **Rivoal** and **Ball** that there is an infinity of irrationals in the sequence $\zeta(2k+1)$ without determining which ones.

To prove the irrationality of certain numbers, we use an interesting result due to **Gauss**.

Theorem

Let : $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ a polynomial of degree n. If $\frac{a}{b}$ is a rational solution with $(a,b) = 1$, then : $a|a_0$ and $b|a_n$.

Proof :

By substituting $\frac{a}{b}$ we find

$$a_n a^n + a_{n-1} b a^{n-1} + \cdots + a_0 b^n = 0$$

or

$$a_n a^n = b(-a_{n-1}a^{n-1} - \cdots - a_0 b^{n-1})$$

It is evident that $b|a_n$. The other elimination gives

$$a_0 b^n = a(-a_n a^{n-1} - \cdots - a_1 b^{n-1})$$

and we have $a|a_0$■

Another formulation of this theorem is that if x_0 is a root of

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

(where $a_n = 1$) then x_0 is either an integer or an irrational.

Example *:*

From above, we can infer that the number $1 - \sqrt{5}$ is irrational, for it is not an integer and it verifies the equation

$$x^2 - 2x - 24 = 0$$

the number $1 + \sqrt{3}$ is irrational , for it is not an integer and verifies the equation

$$x^2 - 2x - 2 = 0$$

As an example, we show the irrationality of certain numbers generated from trigonometric functions:

Example *:*

The number : $sin(20^o)$ is irrational.
to prove this we use some known trigonometric identities $sin(3x) = 3sin(x) - 4sin^3(x)$, putting $x = 20$ we find $64x^6 - 69x^4 + 36x^2 - 3 = 0$.
Suppose now that $sin(10^0)$ is rational. But from the precedent theorem $sin(20^0)$ shold dived and rationnel car $a \nmid b$ ce . so $sin(10^0)$ is irrational.■

As 2023, we do not yet if the following numbers

$$2^e, 2^{log(n)}, 2^\pi, e^e,\ e^{e^e}\ ,\ e^{e^2}, \pi^\pi,,\ \pi^e, \pi^{\sqrt{2}}, \pi^{\pi^2}, \pi^{\pi^\pi}, \pi e,\ \ \pi + e,\ \ , \pi - e,\ log(\pi),\ log\, log(n), log(n)log(k) \ldots$$

are irrationals .

Algebraic numbers:

We will study a new number called *algebraic*. Also we will meet in this chapter for the first time, more complicated numbers than the irrational numbers.

Definition:

We say that a number α is *algebraic* if it is the solution of a polynomial equation

$$P_n(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

where $a_0, \ldots, a_n \in \mathbb{Q}$.

there is not difference if we put $a_0, \ldots, a_n \in \mathbb{Z}$, in the case $P_n(x) \in \mathbb{Z}[x]$ and the former $P_n(x) \in \mathbb{Q}[x]$.

An algebraic number is of *degree n* if it verifies a polynomial equation of degree n :

$$P_n(x) = \sum_0^n a_k x^k = 0.$$

in particular an algebraic of a quadratic equation is quadratic algebraic. If $a_n = 1$ then the polynomial is *monic* and solution is an algebraic *integer* , a concept will be seen in algebraic umber theory. The following are algebraic numbers

$$10^9 \ , \quad i + 5, \qquad \sqrt{6} + 2i \, , \quad 2 + \sqrt[3]{3}$$

we see that an algebraic can be real or complex , the solutions of

$$x^2 - 1 = 0$$

are i and – i. If we note the set of algebraic numbers by the symbol $\mathbb{A}$

$$\mathbb{Q} \subset \mathbb{A} \subset \mathbb{C}$$

It is easy to show that every rational number is algebraic. A rational number is an algebraic number of degree 1.

Let us show that $\sqrt{2} + \sqrt{3}$ is an algebraic number. So $x = \sqrt{2} + \sqrt{3}$ The following

$$x^2 = 5 + 2\sqrt{6}$$

then $x^4 - 10x^2 + 1 = 0$ is the algebraic equation verified by $\sqrt{2} + \sqrt{3}$.

Minimal polynomial of an algebraic number

A *monic* polynomial is a that has $a_n = 1$. If α is an algebraic number, then there is always a unique monic polynomial $p(x)$ with minimal degree, called *minimal polynomial* such that $p(\alpha) = 0$. The other roots of $p(x)$,other than α , are called the *conjugates of α*.

Height of an algebraic number

We say that $p(x)$ is the max of it coefficients

$$h = max(|a_i|)$$

the height of an algebraic number is its minimal polynomial.

Constructing algebraic numbers:

we can construct a lot of algebraic numbers, first all the number of the form

$$a_0 + \sum_{1}^{n} a_k \sqrt{n_k}$$

Are algebraic. Also by trigonometric relations[29] like

$$sin(3x) = 3sin(x) - 4sin^3(x)$$

we put $x = 10$ then we find

$$8x^3 - 6x + 1 = 0$$

Which shows that $sin(10^0)$ is algebraic.

---

[29] These form De Moivre relation in complex analysis.

Numbers that are not algebraic:

A number that is not algebraic is called *transcendental* (appellation due to **Leibnitz**(1704) and **Euler**(1737)). The nature of transcendental numbers is more complicated than algebraic number and even than an irrational number.

Lambert thought that both e and π are transcendantal. **Euler** conjectured that the numbers $log_a(b)$ are transcendental. Already in his book *Introductio* (p.80), **Euler**

> *Since the logarithms of numbers which are not the powers of the base are neither rational nor irrational, it is with justice that they are called transcendental quantities. For this reason, logarithms are said to be transcendental.*

Euler's conjecture turned to be an extremely fruitful one for transcendental number theory. Its proof led to the development of powerful analytic methods in the theory [**Sava**].

It is easy to show that every transcendental number is irrational. So if one has proved that a number α is transcendental, has proven its irrationality too.

Parallellarly we can define an *algebraic function*, a function f is *algebraic* if it verifies a polynomial equation

$$P_n(x)f^n + P_{n-1}(x)f^{n-1} + \cdots + P_1(x)f + P_0(x) = 0$$

Where $P_i(x)$ are polynomials, and a transcendental function does not verify such an equation, functions like

$$sin(x),\ cos(x)\ ,\ 2^x, \Gamma(x) \ldots$$

are not algebraic but transcendental.
In *general* the operations

$$+, \quad -, \quad \times, \quad \div, \quad \sqrt{\ }$$

are algebraic, and the operations

$$\sum_{1}^{\infty} \quad , \quad \int$$

are transcendental, the study of such functions does not concern us here.

Transcendental numbers are more abundant then algebraic ones, in fact algebraic numbers are very rare, for the set of algebraic numbers $\mathbb{A}$ is *denumerable*

$$Card(\mathbb{A}) = \aleph_0$$

a result proved by German Georg **Cantor**(18-191) in 1874, so we can declare :

Heuristically:

if we pick a real number x from the real line we have

$$Probability(\ x\ is\ \boldsymbol{algebraic}) = 0$$

this simple to explain for every rational number

$$a,\overline{bcdef}bcdefbcd\ \ldots$$

which by definition periodic, we can finite number g to turn it in an irrational number

$$a,\overline{bcdef}bcd\boldsymbol{g}efbcd\ \ldots$$

Change the role of g in the thus getting an irrational number, For an y rational we can infinitely irrational number but the opposite is false: we cannot a rational from irrational because e this needs an infinity of operations.

$\mathbb{A}$ lthe set of algebraic numbers, $\mathbb{T}$ the set of transcendental numbers on a

$$\mathbb{R} = \mathbb{Q} \bigcup \mathbb{I} = \mathbb{A} \bigcup \mathbb{T}$$

on the following chart :

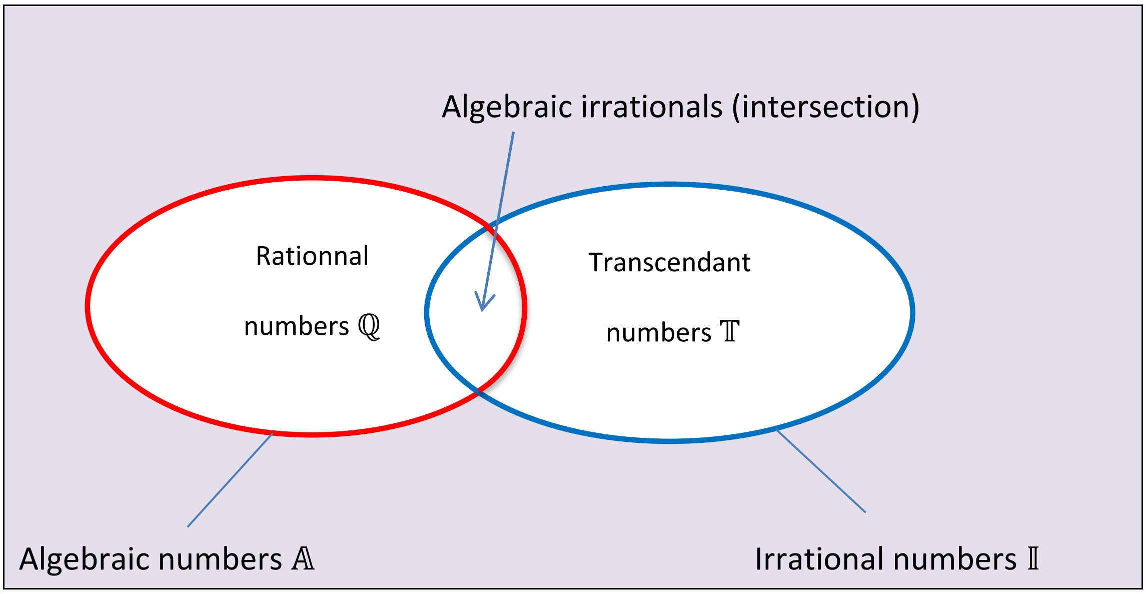


Fig. intersection of the sets of algebraic and irrational numbers.

So

$$Card(\mathbb{T}) = \mathfrak{c}$$

We can now reply to **Kronecker** about the importance of other numbers than the integers

God had created all the numbers for man, to discover and study them in order that he became amazed of His creation, and at the same time be aware of his proper ignorance and weakness.

Besides it is rather simple to construct a transcendental number for example a number that its decimal part contains all integer after the 0:

$$0,12345678910111213141516171819\ldots$$

Called **Mahler** number[30].

Liouville numbers

After we have transcendental numbers following **Hardy**(p. 205) we three:

—prove the existence of transcendental numbers.

—construct examples of such numbers.

—prove that a given number is transcendental.

The theory of transcendental numbers was founded in 1844 by French mathematician Joseph **Liouville**$(1809-1882)$ by proving the existence numbers that are not algebraic, precisely that an irrational algebraic number has a limit of approximation. It is an amazing that algebraic irrational numbers cannot be well *approximated* by rational numbers whereas transcendental numbers can be ,a fact already proved in 1844 by **Liouville**.

a simple *heuristique* idea is to construct a number whose decimal part is not periodic as

$$1{,}01001000100001\ldots$$

---

[30] Also known as *Champernowne number*, to English economist David **Champernowne**(1912-2000). Proved transcendental by the German mathematician Kurt **Mahler**(1903-1988).

Is not rational, **Liouville** established that the following numbers are transcendental

$$\sum_{n=0}^{\infty} \frac{1}{10^{n\,!}}$$

One of the methods for that si its approximation by irrationals with rational , he found *necessary* condition :

Liouville(1844)

A number α is algebraic and equation of degree $n \geq 2$ then there exst a constant c such that for every $\frac{a}{b}$

$$\left|\alpha - \frac{a}{b}\right| > \frac{c}{b^n}$$

And $a, b \in \mathbb{N}^*$

$c >$ real does not depend on b but on α.

The strict $>$ has for cause the n in the denominator, so the degree of the equation and thus the of the algebraic number affect the . For rational α i.e. of degree $n = 1$ the result is false.

What **Liouville** discovered is that algebraic numbers cannot well approximated by rational in a sense that the equation $\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^{n+\epsilon}}$ has only a finite number of rational solutions $\frac{a}{b}$ for any $\epsilon > 0$.

They cannot well approximated even, as we will see, by algebraic numbers. As an example

$$\left|\sqrt{2} - \frac{1}{5}\right| > \frac{c}{25}$$

Proof :

The proof uses the fact that

$$p\left(\frac{a}{b}\right) = a_n\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0$$

$$= \frac{s}{b^n}$$

Where s is an integer . And mean value theorem: $p(x) - p(y) = (x-y)p'(z)$, (polynomial are derivable on $\mathbb{R}$) where $z \in]x, y[$. So we have suppose that algebraic verify the polynomial equation p(x)=0 then

$$\left|p\left(\frac{a}{b}\right) - 0\right| = \left|\frac{s}{b^n}\right| = \left|\alpha - \frac{a}{b}\right| |f'(c)|$$

But

$$\left|\alpha - \frac{a}{b}\right| |f'(c)| = \left|\frac{s}{b^n}\right| \geq \frac{1}{b^n}$$

But

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{|f'(c)|}{b^n}$$

■

So it follows from the above inequality a ***sufficient*** condition on x to be a transcendental number :

Theorem

A number x is a transcendental number iff : $\forall a \in \mathbb{N}^*$, $\exists b, c \in \mathbb{N}^*$

$$\left|x - \frac{a}{b}\right| < \frac{1}{c^a}$$

Liouville asserted that the numbers

$$\sum_{n=0}^{\infty} \frac{1}{a^{n\,!}}$$

when $a \geq 2$ are transcendental, these are Liouville transcendental numbers. the number $\sum_{n=0}^{\infty} \frac{1}{a^{n\,!}}$ is a Liouville number.

Proof :

$$\left|\sum_{n=0}^{\infty} \frac{1}{a^{n\,!}}\right| \leq \frac{1}{a^{n\,!}}(1 + a^{n\,!}$$

So **Liouville** discovered only tiny part of transcendental numbers, his condition was sufficient but not necessary. Although it is not countable, the Liouville transcendental numbers in $\mathbb{R}$ is very small so

Proposition:

Pick a number form $\mathbb{R}$:

$$Probability(\ x\ is\ a\ \boldsymbol{Liouville\ number}) = 0$$

It is to note that π is not a Liouville number as showed by Kurt **Mahler**$(1903 - 1988)$ in 1953

$$\left|\pi - \frac{a}{b}\right| > \frac{1}{p^{42}}$$

So it remains that the exponent δ in $\frac{c}{b^{\delta}}$ is not the best, we look for a lower bound. Liouville inequality we will be ameliorated many occasions, we know Axel **Tue**$(1863 - 1922)$

$$\left|x-\frac{a}{b}\right| \geq \frac{c}{b^{\frac{n}{2}+1+\epsilon}}$$

Tue thus added other transcendental numbers to **Liouville** numbers, and he did more. He this finite solution to prove that the quadratic equation

$$f(x,y) \ = a_n x^n + a_{n-1}x^{n-1}y + \cdots + a \quad y^n = 0$$

has only finite number of solutions.

Then German Claus **Roth**(1925-2015) showed

$$\left|x-\frac{a}{b}\right| \geq \frac{c}{b^{2+\epsilon}}$$

For all $\epsilon > 0$ the best possible as **Dirichlet** showed $\left|x-\frac{a}{b}\right| < \frac{1}{b^2}$.

All needed technics that to find sufficient condition for a polynomial $p(x_1, \ldots, x_n)$ does not vanish at rational arguments. Some methods are *ineffective*: they do not give the solution of inequalities, only majoration.

Hermite breakthrough

After **Liouville** show that e cannot of quadratic, and in 1873 **Hermite** could show that

Proposition:

the famous number e is transcendental.

In fact **Hermite** set basis for future work. He introduced function

$$e^x \int_0^x f(x)e^{-t}\,dt = F(0)e^x - F(x)$$

In 1882, German mathematician **Lindemann**(18-1) developing **Hermite** methods, showed that π is also transcendental. Mainly the equation

$$e^{i\pi} + 1 = 0$$

The solution of Lindemann has given end to a very ancient problem : *squaring of the circle.*

We have two geometric tools *: a e ruler* and a *compass* , drawing a circle of radius 1(unity) can we draw a square whose area is the same area of the disk ? it has been shown tat this to be equivalent to find a square whose side is $\sqrt{\pi}$

We will see that other problem de *constructability* are more in ***Galois*** *theory* , in the algebraic part.

Other result, In 18 **Weierstrass** proved that $log2$ is transcendent.

Algebraic dependence:

Mathematicians have tried to develop general methods to decide if a number is algebraic or transcendental to some ideas.

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

Has for solution algebraic numbers even algebraic non integer. We have already understood the difference between algebraic and transcendental but can a transcendental equation

$$\pi x^3 + log(2)\,x^2 - ex + 1 = 0$$

has algebraic numbers?

This result is known under the name of *fundamental theorem of algebra* (FTA) . **Gauss** has proved in his Doctorate thesis (1799) that

Theorem

every polynomial equation of degree n

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

where the coefficients $a_0, \ldots, a_n$ are complexes, has exactely n complex roots.

bu these cannot be all algebraic because the coefficients are not integers. Another is due to **Gauss** :

Theorem

if the equation

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

Has a complex root $a + ib$ then it has another root $a - ib$.

We take a known concept from linear algebra which is *linear independence*. So we say that the numbers $a_1, \ldots, a_n$ are linearly independent if

$$\sum_{i=1}^{i=n} k_i a_i = 0, \quad then\ k_i = 0$$

Lemma

A number a is transcendental *iff* the numbers $a^0, a^1, \ldots, a^n$ are linearly independent over $\mathbb{Q}$ for every n.

In fact in his work on transcendence of the number e, **Hermite** proved that the for $n \geq 1$ the numbers

$$1, e\ , e^2, \dots, e^n$$

are linearly independent over $\mathbb{Q}$.

Linear independence(over $\mathbb{Q}$)

algebraic independence(linearly independent over $\mathbb{A}$)

We can find linear independence with the Wronskian[31]. We say that $f_1, \dots, f_n$ are linearly independent if the

$$W(f_1, f_2, \dots) = \begin{vmatrix} f & f & f \\ f & & \end{vmatrix} = 0$$

Ff

lemma

if f_1 and f_2 are linearly dependent $\Longrightarrow$: $W(f_1, f_2, \dots) = 0$.

but $\Longleftarrow$ may be false (there is no equivalence $\not\Leftarrow$) . In 1889 **Peano**$(18-19)$ gave an example : x^2 and $x|x|$.

Example

Calculate the Wronskian of: $(cos(x)\ , sin(x))$

and another new concept :

Definition

---

[31] To Polish mathematician Joseph **Wronski**(1776-1853) who

We say that a set of numbers $(a_1, \dots, a_n)$ are *algebraically* *independent* if there exists a polynomial of several variables $p(x_1, \dots, x_n)$ we have

$$p(a_1, \dots, a_n) \neq 0$$

Every transcendental number is algebraically independent ($n = 1$), and any set of algebraic numbers : $a_1, \dots, a_n$ are algebraically dependent. Any set of numbers $a_1, \dots, a_n$ containing at least one algebraic numbers is algebraically dependent. So we take very valuable information when every number in $a_1, \dots, a_n$ is transcendental. We that for function

But, there are numbers although transcendental, are algebraically dependent . For instance, the two transcendental numbers : $\sqrt{\pi}$ and $\pi + 1$ are algebraically *dependent* for they verify the polynomial equation : $2x^2 - 2y + 1 = 0$. Also $sin^2(1) + cos^2(1) - 1 = 0$ and both $sin(1)$ and $cos(1)$ are transcendental.

Even old numbers like π and e continue to vex mathematicians, for we do not know if there exist natural numbers k_1, k_2 such that

$$\pi^{k_1} = e^{k_2}$$

if so, they are algebraically independent.

Theorem

Let $\alpha_1, \dots, \alpha_n$ be n algebraic numbers which are algebraically independent, then $p(\alpha_1, \dots, \alpha_n)$ is transcendental.

One of the first results to the relation between linear dependence and algebraic dependence was:

Weierstrass theorem(1885)

Let $a_1, \dots, a_n$ n distinct algebraic numbers which are linearly independent, then $e^{a_1}, \dots, e^{a_n}$ are algebraically independent.

The result was first in 1882 by **Lindeman** then proved by **Weierstrass**. The theorem tells us that if a_i are algebraic then e^{a_i} cannot all be rational, this implies that e is transcendental (think of the case $k_1 e^{a_1} = 0$ and $a_1 = 1$). Both result of are special cases $n = 1$ of Weierstrass theorem.

Lindeman proved that e^{α} (α algebraic)is transcendental. It seems simpler to prove that numbers are algebraic independent than to show that they are transcendental. Weierstrass theorem was a beginning of methodology of searching of transcendental numbers. In 1996, Russian Yuri **Nesterenko** (born in 1946) showed that π and π^e are algebraically independent.

Hilbert's question

Diophantine approximation:

the problem of the irrationality of some special numbers has preoccupied many mathematicians, and **Hilbert** in his *seventh* problem (1900), seek the determination of the nature numbers of the form

$$\alpha^{\beta}$$

Where α is algebraic and β algebraic irrational. This goes back to **Euler**, we know if the log is in base α and β then $log\beta$ so

$$\frac{log()}{log()}$$

As follows :

Hermite's arithmetical theorems on the exponential function and their extension by ***Lindeman*** *are certain of the admiration of all generations of mathematicians. Thus* *the task at once presents itself to penetrate further along the path here entered, as A.* ***Hurwitz*** *has already done in two interesting papers*[*]*," Ueber arithmetische Eigenschaften gewisser transzndnter Function." I should like, therefore, to sketch a class of problems which, in my opinion, should be attacked as here next in order. That certain special transcendental functions, important in analysis, take algebraic values for certain algebraic arguments seems to us particularly remarkable and worthy of thorough investigation. Indeed, we expect transcendental functions to assume, in general, transcendental values for even algebraic arguments; and, although it is well known that there exist integral transcendental functions which even have rational vales for all algebraic arguments, we shall still consider it highly probable that the exponential function* $e^{i\pi z}$ *for example, which evidently has algebraic values for all rational arguments z, will on the other hand always take transcendental values for irrational algebraic values of the argument* z*. We can also give this statement a geometrical form, as follows:*

If, in a isosceles triangle, the ratio of the base angle to the angle at the vertex be algebraic but not rational, the ratio between base and side is always transcendental.

In spite of the simplicity of this statement and of its similarity to the problems solved by ***Hermite*** *and* ***Lindmann****, I consider the proof of this theorem very difficult; as also the proof that:*

The expression α^{β} *, for an algebraic base* α *and an irrational algebraic exponent* β *e.g., the number* $2^{\sqrt{2}}$ *or* $e^{\pi} = i^{-2i}$ *, always represents a transcendental or at least an irrational number.*

It is certain that the solution of these and similar problems must lead us to entirely new methods and to a new insight into the nature of special irrational and transcendental numbers.

Siegel (1896-198) began a new branch in searching transcendental number, number that are values of certain complicated functions. He proved the result:

Siegel theorem(1929)

The **Bessel** function $J_0(x)$ gives transcendental numbers when x are algebraic.

---

[*] Math, Annalen, vols. 22, 32 (1883, 1888).

The function $J_0(x)$ is the solution of **Bessel** differential equation

$$x^2y'' + xy' + (x^2 - \alpha^2)y = 0$$

Work by norvegien mathématicien **Thue** (18-19) in 1909 et le mathématicien allemand **Siegel** en 1931 ont fait dans la même vois est le critère d'approximation mais avant on le lemme de **Siegel**

__Siegel__'s lemma__(1929) :__

soit un système de mm équations linéaires de n inconnus de coefficients entiers, avec $n > m$ et x_0 une solution alors la solution du système on

$$x_0 < (nb)^{\frac{m}{n}-m}$$

où $b = max|a_{ij}|$

Ce lemme de **Siegel** permet

Then Russian A.O. **Guelfond** $(1906 - 1968)$ a special case of the problem:

Guelfond(1929)

If the β is is algebraic complex then α^β is transcendental.

This enabled him to prove that the numbers: e^π and $e^{-\pi}$ are transcendental for $e^\pi = (-1)^{-i}$ and $e^{-\pi} = i^{2i}$ and both I and 2i are algebraic.

In 1930 another Russian Rodion **Kuzmin**$(1891 - 1949)$ proved another

Kuzmin(1930)

If β is quadratic algebraic then α^{β} is transcendental.

Only a special case so numbers

$$2^{\sqrt{3}+\sqrt{2}}$$

Afterwards with the aid of the lemma, A.O. **Guelfond** $(1906-1968)$ and **Schneider** $(1911-1988)$ (**Siegel**'s student) independently proved the following result which solve the problem posed by **Hilbert** :

Theorem (1934)

if α et β are two algebraic numbers irrationals then α^{β} is transcendental.

But the theorem says nothing about the numbers

$$2^{\pi}, \pi^{e}, \pi^{\sqrt{2}}, \dots$$

their result was ameliorated by **Roth** :

this result is sometimes named **Roth**-**Thue**-**Siegel** theorem.

Logarithmic forms and Baker theorem

in 196 **Baker** has generalized the result :

Baker theorem(196)

If $\alpha_1 \dots \alpha_n$ and $\beta_1 \dots \beta_n$ are algebraic numbers and then the numbers

$$\beta_1 \, log(\alpha_1), \dots, \beta_n log(\alpha_n)$$

are independent over $\mathbb{A}$

This mean that

$$\beta_1\, log(\alpha_1) + \cdots + \beta_n log(\alpha_n) \neq 0$$

Baker's theorem is seen as a big generalization, the Guelford-Schneider and de Hermite-Lindemann theorems are just special cases. So when $n = 1$ we find the Hermite-Lindemann-Weierstrass and when $n = 2$ we find the Guelfond-Schneider. Form **Baker** that numbers as

$$e2\sqrt{2,}\ ,\pi + \log(\sqrt{\quad}$$

Are transcendental

Algebraic consideration

We can now formulate what we have already in an algebraic language. An algebraic number is a number over $\mathbb{Q}$. So an equation

$$x^2 + 3x + 1 = 0$$

Gives numbers are of the form

$$a + b\sqrt{5}$$

if we solution which are not in $\mathbb{Q}$. So we see $\mathbb{Q}$ is a field as $\mathbb{Q} \subset \mathbb{R}$. in We can an extension of this tm with $\mathbb{R}$, And also it is a field. $\mathbb{T}$ is not a filed. Extension of field has for origin solution of algebraic equation $p(x) = 0$.

But if consider solution in $\mathbb{R}$ only we lose a lot of algebraic numbers. $\mathbb{C}$, one of the features of $\mathbb{C}$ has a it is *algebraically close* means that a any equation with coefficients in $\mathbb{C}$, are in $\mathbb{C}$. The set $\mathbb{Q}$ has not this propriety, the equation

$$x^2 + x + 1 = 0$$

Has coefficients in $\mathbb{Q}$ but its two solutions are in $\mathbb{C}$. so $\mathbb{Q}$ is not algebraically close, also $\mathbb{R}$ is not algebraically close. Both extension of $\mathbb{C}$ and also three fields $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. The set $\mathbb{Q}$ has not a field in it , it is a *prime field*. Algebraic numbers $\mathbb{A}$ is the closure of $\mathbb{Q}$ in $\mathbb{C}$, we that by writing

$$\mathbb{A} = \overline{\mathbb{Q}}$$

it is an algebraic closure. So has two extension the second is the more interesting.

Degree of transcendence.

As $k = \mathbb{Q} \subset K = \mathbb{C}$ is seen a filed extension of $\mathbb{C}$, every transcendental number is algebraically independent over $\mathbb{Q}$, and any set of algebraic numbers : $a_1, \dots, a_n$ are algebraically dependent over $\mathbb{Q}$. Any set of numbers $a_1, \dots, a_n$ containing at least one algebraic numbers is algebraically dependent. B

Exercises

1) show that $0.\overline{123456789}\dots$ is a rational number.
1) show that the number : $2.01269001212\overline{356}$..... is rational.
1) let $x \notin \mathbb{Q}$, show that its decimal part also $\notin \mathbb{Q}$.
1) prove that there are infinitely many irrational numbers in $\mathbb{R}$.
1) prove that there are infinitely many irrationals in any interval $[n, n+1]$.
Give a dense set of rational in $[n, n+1]$.

1) prove that there are infinitely many irrational numbers in any interval $]a, b[$ such that a and b are rational. Give a dense set of rational in$]a, b[$.

1) show that there are infinitely many irrationals in any $]a, b[$ were a and b are irrational.

1) Prove that there are infinitely many irrational numbers in the intervals

$$]e, \pi[, \qquad]e, 3[, \qquad]3, \pi[$$

1) show that : $\sqrt{3} \notin \mathbb{Q}$.

1) show that : $\sqrt[3]{2}$ is irrational.

1) show that : $\sqrt{6} \notin \mathbb{Q}$. Infer that $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

1) show that $\sqrt{2(2n+1)}$ is irrational for every $n \in \mathbb{N}$.

1) is $\sqrt{2n}$ irrational when $n \in \mathbb{N}$?

1) show that if n is square free then : $\sqrt{n} \notin \mathbb{Q}$.

1) show that if $a^n \notin \mathbb{Q}$ then $a \notin \mathbb{Q}$.

1) let n not a square and $a, b \in \mathbb{Q}$, show that $a + b\sqrt{n} \notin \mathbb{Q}$.

1) prove the equivalence : a is rational $\Leftrightarrow$ a has a periodique decimal part**.**

1) let a, b two irrationals, what can you say about : $a + b$, ab and $\frac{1}{a}$?

1) let a a rational and b an irrational, what can we say about : $a + b$, ab , $\frac{1}{ab}$?

1) show that the equation : $x^2 + x + 1 = 0$ has no rational solutions.

1) show there are infinitely many x such that $cos(x), sin(x) \in \mathbb{Q}$.

1) show that if $cos(2x) \notin \mathbb{Q}$, then $sin(x) , cos(x) \notin \mathbb{Q}$.

1) show that if $cos(2x) \notin \mathbb{Q}$, then $tan(x) \notin \mathbb{Q}$ (use $1 + tan^2(x) = \frac{1}{\cos^2(x)}$).

1) find the series

$$\pi = \sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1}$$

(use the antederivative of $arctan(x)$).

1) show that $\frac{\log(2)}{\log(3)}$ is irrational.

1) show that $\frac{\log(n+1)}{\log(n)}$ is irrational.

1) let p_1, p_2 two primes, show that $\frac{\log(p_1)}{\log(p_2)}$ is irrational.

1) let $(a, b) = 1$, show that $\frac{\log(a)}{\log(b)}$ is irrational.

1) write the following numbers as infinite series

$$e^{\pi}, cos(2) , sin(1)$$

1) let $a \in \mathbb{N}^*$, show that if : $\sqrt{a}^{\sqrt{a}}$ is irrational then : $\sqrt{a}$ is also irrational.

1) give two irrational numbers a and b such that a^b is rational. Show that there are infinitely many of them.

1) Are there two different irrational a and b such that : $\frac{a}{b} \in \mathbb{Z}$?

1) show that if $n \in \mathbb{N}$ and k is not an n^{th} power , then $\sqrt[n]{k}$ is irrational.

1) show that we can have the previous result from **Gauss** theorem.

1) let C_B be **Brun**'s constant, show that if C_B is irrationnal then the set of twin primes is infinite.

1) let $\alpha \notin \mathbb{Q}$, show that $\sqrt{\alpha} \notin \mathbb{Q}$.

1) show that if α is irrational then $\sqrt[n]{\alpha}$ is irrational.

1) le α and β two irrationals, show that if $\alpha + \beta$ are rational then $\alpha - \beta$ and $\alpha + 2\,\beta$ are irrational.

1) let $\frac{a}{b}$ be an irreducible fraction, show that $\sqrt{\frac{a}{b}}$ is irrational.

1) in algebraic number defined as a solution of a polynomial equation of finite degree n, does it work if n is infinite?

1) is there $n \in \mathbb{Z}$ such that $cos(n) = 0$? $tan(n) = 0$?

1) show that at least one of the two numbers $e + \pi$ and $e - \pi$ is irrational.

1) show that $log_{10}(3) \notin \mathbb{Q}$.

1) find when is $log_n(m) \notin \mathbb{Q}$.

1) show that if : $cos(2x)$ est irrational then $cos(x)$, $sin(x)$ and $tan(x)$ are irrationals.

1) show that if : $sin(2x)$ est irrationnel then at least $cos(x)$, $sin(x)$ is irrational.

1) show that π^n and e^n are irrational.

1) show that $log(2)$ is irrational.

1) show that $log(n)$ is irrational, for every $\mathbb{Z} \ni n > 1$.

1) show that $e + \sqrt[n]{a}$ and $\pi + \sqrt[n]{a}$ are irrational.

1) show that a is a rational is algebraic integer iff $a \in \mathbb{Z}$.

1) **Euler** found that : $\zeta(2k) = \frac{(2\pi)^{2k}(-1)^{k+1}B_{2k}}{2(2k)\,!}$, show that they are irrationals.

1) let $r \in \mathbb{Q}$, show that π^r and e^r are irrational.

1) show that $\sum_{n\geq 1}\frac{1}{2^{n!}}$, $\sum_{n=1}^{+\infty}\frac{n}{10^{n!}}$ converge.

1) Show that $\sum_{n=1}^{+\infty}\frac{1}{10^{n}}$ converges. Write its decimal part.

1) Show that every number rational is algebraic and every transcendental number is irrational.

1) pick up a number form $\mathbb{R}$, what is probity irrational ?transcendental?

1) show that : $i+\sqrt{2}$ is algebraic.

1) show that : $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is algebraic.

1) if $\sqrt{d}\notin\mathbb{Q}$, show that 1 and $\sqrt{d}$ are linearly independent over $\mathbb{Q}$.

1) calculate the Wronskian of two functions $(x+1\ ,x-1)$ are they dependent?

1) show that $(1,cos(2x)\ ,cos^2(x))$ are not dependent.

1) show that : $(e^{-x}\ ,e^{x})$ are linearly independent over $\mathbb{Q}$.

1) solve the differential system for t

$$\begin{cases} x'=y+z \\ y'=x+z \\ z'=x+y \end{cases}$$

calculate the **Wronksian.**

1) Show that $cos(x)$ and $sin(x)$ are algebraically dependent.

1) show that $sin(\pi+e)$ and $cos(\pi+e)\notin\mathbb{Q}$.

1) show that $\sum_{0}\frac{1}{(2n+1)^{2k}}$ cannot be rational for all $k\geq 1$.

1) Show that if $\alpha,\beta\in\mathbb{A}$, then : $\alpha+\beta,\alpha-\beta,\frac{\alpha}{\beta}(\alpha\neq 0)\in\mathbb{A}$. .

1) let $r\in\mathbb{Q}$. Show that if $\alpha\in\mathbb{A}$ then $r\alpha\in\mathbb{A}$.

1) what if α and β are algebraic, is then $\beta\alpha$ algebraic?

1)) let $r\in\mathbb{Q}$. Show that if $\alpha\in\mathbb{T}$, then $r\alpha\in\mathbb{T}$.

1) what if α and β are transcendental, is then $\beta\alpha$ transcendental?

1) show that any algebraic number is algebraically dependent.

1) show that a set of numbers containing an algebraic are algebraically dependent.

1) show that every transcendental number is algebraically independent.

1) show that the algebraic numbers $\alpha_1,\dots,\alpha_n$ are algebraically dependents.

1) show that the number α is transcendental $1,\alpha,\alpha^2,\dots,\alpha^n$ are linearly independent over $\mathbb{Q}$.

1) let α be an integer and β irrational, is α^{β} algebraic ?

1) let α and β rational numbers, is α^{β} algebraic ?

1) if α is algebraic and β algebraic rational, what about α^{β} ?

1) show that l$og(\frac{2}{3}) \notin \mathbb{Q}$.

1) show that the number $13e^{14} + 5e^{6} - 1$ is irrational.

1) show that le number $3\pi^{27} - 2\pi^{3} - 2\pi^{2} + 12$ is irrational.

1) is the number $e^{9} + 5e^{6} - 3i$ rational ?

1) show that : α is algebraic $\Leftrightarrow$ $\frac{1}{\alpha}$ is algebraic.

1) show that : α is transcendental $\Leftrightarrow$ $\frac{1}{\alpha}$ is transcendental.

1) let $a \in \mathbb{Q}$, show that : $e + k$ and $\pi + k$ are transcendental.

1) show that the sum of an algebraic and a transcendental is transcendental.

1) show that the product of an algebraic and a transcendental is transcendental.

1) show that $\mathbb{R}$ is not algebraically close.

1) show that $\mathbb{T}$ is not a filed.

Open problems

The problems proceeded by the sign (*) are mine, as far as I know, I have not found them in the literature.

1) is there an odd perfect number ? (Antiquity)
2) **Goldbach** conjecture (1743), (8^{th} **Hilbert**'s problem)
3) Idoneal numbers conjecture.
4) congruent number problem: how can we know that a given integer(rational) is a congruent number?
5) is there a formula that gives the number of primitive roots modulo n ?
6) **Gauss** and **Artin's** conjectures on primitive roots.
7) twins conjecture : p_n, p_{n+1} (8^{th} problem of **Hilbert**)
8) Brocard's problem: a square of the form $n! + 1$ when $n > 7$?
9) **Lemoine** conjecture (1895).
10) **Grimm** conjecture : if $a_1, \dots, a_k$ then $p_i | a_i$
11) infinitude of primes of the form : $n^2 + 1$ (**Hardy** and **Littlewood** 1922)
12) **Lehmer's** problem (1932): find a composite n such that $\varphi(n) | n - 1$?
13) **Chirmicael** conjecture (1933): find a composite n such that $\varphi(n) | n - 1$?
14) are there infinitely many n_1, n_2 such that $\varphi(n_1) = \varphi(n_2)$?
14) The "$3n + 1$ $conjecture$" , known also under the name: **Collatz** conjecture (1937).
15) every sufficiently large integer is the sum of 4 nonnegative cubes.
16) are there infinitely many primes of the form n^2 -2?
17) are there infinitely many primes of the form $n^2 < p < (n + 1)^2$(conjecture of **Lagrange**)
18) are there infinitely many primes in a polynomial $ax^2 + bx + c$ $(a \neq 0)$ (see [H] p.23)
19) is there infinitely many of **Germain** primes : $2p + 1$?

20) consider the sequence: $s_n = \sum_{i=1}^{n} p_i$. Is there infinity many primes in s_n ?

21) infinitely many primes of the form : $2 \times 3 \times 5 \times 7 \ldots \times p_n + 1$

22) are there infinity of primes $2^p - 1$ (**Mersenne** numbers)

23) is there infinitely many composite numbers $2^p - 1$ (**Mersenne** non primes)

2) is there infinitely many premiers de Fermat $2^{2^n} - 1$?

2) is there infinitly many of composite Fermat numbers $2^{2^n} - 1$?

2) ∀ n, ∃ p_1 et p_2 such that : $n = p_2 - p_1$ (Green-Tao ?) ?

2) est ce qu'il existe infinité de racines primitives ?(Artin conjecture)

2) the nature of the Euler-M constant:

$$\gamma = \lim_{n \to \infty} \sum_{n \geq 1} (\frac{1}{n} - logn)$$

3) Are the numbers :

$\frac{e}{\pi}$, π^{π} , e^e , $e + \pi$, $e - \pi$, π^e, a^{π} , a^e $(a \neq 1)$, $log\pi$(or $e\pi$),

2^e , $\pi^{\sqrt{2}}$ irrational (transcendental) ?

1) the nature of the numbers $\zeta(2n+1), n \geq 2$.

1) the nature of the **Catalan**'s constant.

1) algebraic independence of π and e.

1) **Schanuel** conjecture.

1) the ABC conjecture.

1) **Beal** conjecture (1993).

***1)** are there infinitely many prime decimal inverses (like : $13 - 31$, $167 - 761$)

***1)** Are there infinitely many primes of the form $2^{n!} + 1$?

***1)** is there an infinitely of squares in the sequences : $\sum_{i=1}^{n} p_i$?

***1)** infinitude of primes of the form : $(n\,! - 1, n! + 1)$?

***1)** infinitude of primes of the form: $(\ n! - n - 1 \ , \ n! + n + 1 \ )$?

***1)** $\exists n_0 \in \mathbb{N}$, $\forall k \in \mathbb{N} : n \geq n_0 \implies \exists n : \tau(n) = k$

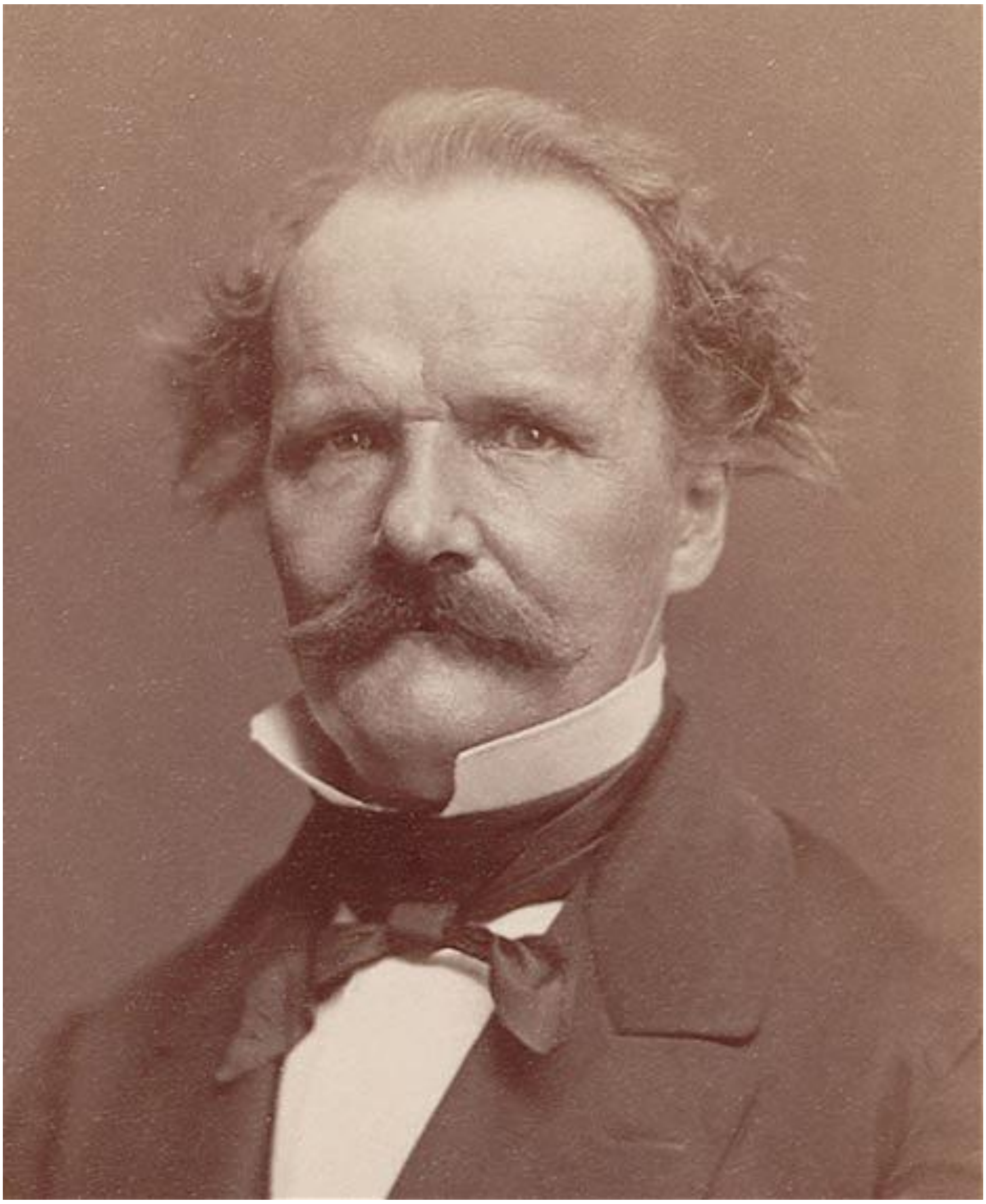
***1)** exclude n from $\sigma(n)$: what is the value of

$$\lim_{n \to \infty} \sigma(\sigma(\ldots \sigma(n)))$$

***1)** let $p! = 2 \times 3 \times 5 \times \ldots \times p$, noted also $p^{\#}$. Are there infinitely many squares of the form $p^{\#} - 1$?

Second part

Algebraic number Theory



Ernest **Kummer**

Chapter 1

Origins of algebraic number theory

Algebraic number theory has been founded by mathematicians following their efforts among others, to prove the reciprocity laws (quadratic,…), study of quadratic forms and especially to solve le Fermat's Last Theorem (FLT). More important in this context, through their works on problems of number theory, mathematicians have given a new meaning particularly to the concepts of : *number*, *integer* and *algebraic operations*.

Cyclotomic numbers :

Complex numbers played an important in the genesis the algebraic aspect of number theory, already **Gauss** has proved in his Doctorat thesis (1799) that every polynomial equation of degree n

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

where the coefficients $a_0, \dots, a_n$ sont complexes, has exactly n complex roots, prouvant ainsi une old conjecture stated by the french mathematicien **Girard** (1595-1632) in 1629. This result is known under the name of *fundamental theorem of algebra* (FTA) .

a special equation of the FTA is the equation

$$x^n - 1 = 0$$

has been particularly well studied. It is called cyclotomic equation because its solutions which are the roots of 1 are situated on the circle or radius 1 or equivatly $|z| = 1$, d'où le nom de leur equation « *cyclotomique equation* », from *cyclo :* 'circle' and *tomae* : 'partager'.

Definition:

we say that a complex number $\zeta = a + ib$ is a *nième* root de 1 , if there exists an integer n such that

$$(a + ib)^{\,n} = 1$$

In his book *Disquisitiones Arithmeticae* , **Gauss** treated the equation of the form

$$x^p - 1 = 0$$

And succeded to solve it after many attempts of mathematicians before him. The solution are complex numbers ζ_k de la forme

$$\zeta_k = cos\frac{2k\pi}{p} + isin\frac{2k\pi}{p} = e^{i(2k\pi)/p}$$

Called the $p^{\text{èmes}}$ roots of unity and verify the quation

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$$

Because the cyclotomic equation $x^p - 1 = 0$ is also equivalent to the equation

$$(x-1)(x^{p-1} + x^{p-2} + \cdots + 1) = 0$$

The number ζ is a primitive root of 1

Definition :

the $n^{\text{ème}}$ root de l'unité ζ is called *primitive* if n est le plus petit entier positive tel que $\zeta^n = 1$

Example:

for the cyclotomic equation $x^3 - 1 = 0$, the roots are

$$1, \qquad \frac{1}{2} + i\frac{\sqrt{3}}{2}, \qquad \frac{1}{2} - i\frac{\sqrt{3}}{2}$$

If we know ζ on trouve les deux autres qui sont 1 and ζ^2. Alors ζet ζ^2 sont les racines primitives. On a alors le following result

Theorem:

the number of primitives roots of $x^n = 1$ is $\varphi(n)$.

In the precedent example: $\varphi(3) = 2$ primitive roots, they are

$$\frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{and} \quad \frac{1}{2} - i\frac{\sqrt{3}}{2}$$

which correspond to (ζ and ζ^2).
Thus **Gauss** gave a solution to an ancient problem called *construction of the regular polygons*. In fact, **Gauss** showed that the construction was possible if n is a prime of **Fermat** $p = F_n = 2^{2^n} + 1$ (pure coïncidence) or the product of two distinct Fermat primes.

Since $\varphi(p) = p - 1$,there are numbers

$$1\,,\ \zeta,\ \zeta^2, \dots,\ \zeta^{p-1}$$

which will be very important in this theory , occur naturally in the factorization

$$x^p\ -\ 1 = (x-1)\ \times (x-\ \zeta)\ \times \dots \times (x-\ \zeta^{\,p-1})$$

3) The reciprocity law:

Gauss(1831) also used complex numbers in his study of the law of quadratic reciprcity

$$x^2 \equiv p\ mod(q)$$

where he introduced the numbers

$$a + ib$$

where a et b ∈ ℤ. These numbers are called *Gaussian integers* , a name to them from ℚ which we call we will the *rational integers*.

Gauss got the idea to apply the Euclidian division from theory of divisibility to these numbers, for two Gaussian integers we have

$$\alpha = \beta\gamma + \delta$$

And thus has and Euclidian algorithm, Gauss

Consider the numbers $a + ib$ *as* ***integers***.

Gauss integers from reciprocity law were of the form,

$$a_0 + a_1\zeta^n + \cdots + a_{p-1}\zeta^{p-1}$$

and attacked the cubic reciprocity law $n = 3$, he introduced the numbres

$$a + b\zeta$$

où les nombres complexes ζ = $e^{(2i\pi)/3}$ are the 3^{eme} roots of unity et a et $b \in \mathbb{Z}$.

Gauss also wrote two papers (1828 and 1832) on biquadratic reciprocity

$$x^4 \equiv p \; mod \; q$$

3) The Fermat's Last Theorem :

Fermat's Last Theorem (FLT) was a conjecture due to **Fermat** which says that the equation

$$x^n + y^n = z^n$$

has no positive integer solutions (> 0) when $n > 2$. The equation (1) is a particular case of what we name the algebraic *equations* or *polynomials* equations such

$$x^2 + x = 0, \qquad yx^3 + y^{10} = z^2, \qquad \ldots$$

which played a major role in the creation of modern algebra. In particular le FLT est appelé équation *Diophantine* which we have seen before. For $n = 2$ the equation

$$x^2 + y^2 = z^2$$

has infinitely many solutions, the famous *primitive triples* $(2ab, a^2 - b^2, a^2 + b^2)$ where a and b are relatively prime.

Fermat proved the case $n = 4$ of FLT (apparently the sole proof of all his observations) by showing that

$$x^4 + y^4$$

Cannot be a square, by using his *infinite descent method*. But mathematicians after him concluded that :

Theorem :

to prove the **Fermat** Last Theorem, it suffices to prove there no solutions when the exposant $n > 2$ is a prime number p.

For $n = 3$ the proof was difficult and even the great **Euler** struggled with it to give only an erroneous proof. But **Euler** was the first mathematician to have a new genius idea, namely to use irrational and complex numbers in the solution of (FLT). In order to prove the theorem for $n = 3$, **Euler** wrote the decomposition

$$x^3 = (z + y)(z^2 - zy + y^2) = (z + y)(z + \zeta y)(z + \zeta^2 y)$$

Where ζ is the 3^{rd} root of unity, he used infinite descent method : suppose there exists a solution (x, y, z) then at least l'un des x , y, z is an even integer. Euler arrived to the conclusion that equation is equivalent to

$$2p(p^2 + 3q^2) = cube$$

And if we write le term between parenthèsese

$$p^2 \ + \ 3q^2 = (x + y\sqrt{-3}) \times (x - y\sqrt{-3})$$

Alors si p et q sont premiers ente eux alors les nombres $(x + y\sqrt{-3})$ et $(x - y\sqrt{-3})$ sont eux même des cubes, for if $a \times b$ est un cube and $(a, b) = 1$ then alors a et b sont eux même des cubes d'où une contradiction. See [Ed] for more discussion.
the new idea and originelle that Euler had before Gauss was divisibility

*Consider the numbers $(x + y\sqrt{-3})$ and $(x - y\sqrt{-3})$ as **integers**.*

Euler assuma que la factorisation de $x^p + y^p$ in prime factors premiers was unique, mais il avait de la chance car aujourd'hui on sait que ce n'est pas toujours vrai. En fait l'unicité de factorisation en des facteurs premiers était démontrée vraie only for $n = 2,3$. **Gauss** proved unicity of factorization for $n = \ 4$ and gave a proof of FLT for $n = 3,4$ by considering the numbers

$$\frac{a}{2} + \frac{b}{2}\sqrt{-3}$$

In this, the numbers whose product is 1 , (that is are divisors of 1) are not taken into account, because they have no role, as the two -1 and 1 in the divisibility in $\mathbb{Z}$, we will see that such numbers are called *units*.

In 1769, **Lagrange** wrote

> *" ...M. de **Fermat** prétend, dans ses remarques sur **Diophante** , avoir démontré en général ce théorème que l'équation $r^n + s^n = q^n$ n'est jamais resoluble d'une manière rationnelle lorsque n surpasse 2; mais ce Savant ne nous a pas laissé sa démonstration, et il ne parait pas que personne l'ait encore trouvé jusqu' à présent . M. **Euler** a, à la vérité, démontré ce théorème dans le cas de n=3 et de n=4, par une analyse particulière et très ingénieuse mais ne parait pas applicable en général à tous les autres cas; ainsi, ce théorème est un de ceux qui restent encore à démontrer, et qui méritent le plus l'attention des Géomètres."*

After **Euler**, the history of the solution of FLT for some other prime exponents p was as follows :

$n = 5$ (**Dirichlet**(1825) and **Legendre**(1828))
$n = 14$ (**Dirichlet** 1832, échec with $n = 7$)
$n = 7$ (**Lamé** 1839)

all these solutions depended on a factorization of $x^p + y^p$ in two complex factors , for a factorization with *integer* coefficients does not exist for $p > 3$. then came the work of French mathematician Sophie **Germain** (1776-1831). **Germain** gave a proof for $n = 5$ and stated her theorem under its general form was éstablished :

Theorem (18) :

If q is an odd prime and $p = 2q + 1$ a prime then the equation $x^p + y^p = z^p$ implies that p divides $x, y \ or \ z$.

this result a classified le problem of FGT into two cases :

$i)$ none of x, y, z is divided by p $(or\colon\ p \nmid xyz)$
$ii)$ only one of x, y, z is divided by p ($or\colon\ p|xyz$, with $(x, y, z) = 1$)

3) Kummer and ideal numbers :

In 1847 , the French mathematician **Lamé**(1-18) proposed a proof of FLT by introducing the factorization

$$x^p + y^p = (x+y) \times (x + \zeta\, y) \times \ldots \times (x + \zeta^{\,p-1} y)$$

where $\zeta^{\,p} = 1$ got like this: since

$$t^p - 1 = (t-1) \times (t - \zeta) \times \ldots \times (t - \zeta^{\,p-1})$$

Putting $t = -\frac{x}{y}$ and multiplying by $-y^n$ we get the needed equation.

Lamé reasoned like this : if

$$(x+y) \times (x + \zeta\, y) \times \ldots \times (x + \zeta^{\,p-1} y) = z^p$$

and since the factors $(x+y)$, ..., $(x - \zeta^{\,p-1} y)$ are coprime (for x and y are coprime) then these factors would be of the form ${u_i}^p$ which gives a contradiction with $(x, y, z) = 1$. In fact **Lamé** made the same inadvertance qu'Euler, croyait que l'unicité de factorisation of cyclotomic numbers was unique for every n. But if **Euler** had a chance, for the unicity of factorization was true for $n = 3$, **Lamé** not.

In another field initiated by **Gauss** then **Jacobi**, **Kummer** was interested in the law of reciprocity. In a lettre to **Liouville** en 1847, il affirma que le reasonning of **Lamé** was false. The factors

$$(x+y),\ \ (x - \zeta y),\ \ \ldots\ ,\ (x - \zeta^{p-1} y)$$

Could not be always coprime. **Kummer** considered complex numbers looking like the factors $x-\zeta^{p-1}y$: let p be a prime, we consider the equation

$$f(\zeta)=a_0+\ a_1\zeta+\cdots+a_{p-1}\zeta^{p-1}$$

where $a_0, \ldots, a_{p-1}$ are integers and ζ is the p^{eme}root of unity ($\zeta^p=1$) , the number $f(\zeta)$ resulting from this operation is called a *cyclotomic integer*. We have seen that Gauss introduced two of them the *Gaussian integers*

$$a+bi$$

In case reciprocity $n=2$ ($i^2=1$), and

$$a+b\zeta$$

In case reciprocity $n=3$ ($\zeta^3=1$)

They are set of numbers generated by the roots of unity 1 , we can prove the curious propriety : if k is an integer then

$$(a_0+k)+\ (a_1+k)\zeta+\cdots+(a_{p-1}+k)\zeta^{p-1}=a_0+\ a_1\zeta+\cdots+a_{p-1}\zeta^{p-1}$$

Kummer found some facts about them

i) there are cyclotomic integrs such that $\alpha|\beta$ and $\alpha|\beta$ without $\alpha\neq\beta$, we say that α is *associated* to β and we note $\alpha\sim\beta$

ii) if $\alpha|1$, α is called a *unit* there are infinitely many units

The problems posed :

Question:

i) when is a cyclotomic number α prime?

The solution is define it like in $\mathbb{Z}$

A α is prime if it is divisible only by unites(1 in) or $\alpha \sim \beta$ ($n|n$ like in $\mathbb{Z}$)

iii) **Kummer** found a very strange propriety that does not work like in integers $\mathbb{Z}$: let $\alpha_1, \dots, \alpha_k$ and $\beta_1, \dots, \beta_l$ are cyclotomic primes but

$$\alpha_1 \times \dots \times \alpha_k = \beta_1 \times \dots \times \beta_l$$

the unique factorization in primes is not unique!!! Another propriety known in $\mathbb{Z}$, but does not work hereis :

$$\text{if is a prime then : } \alpha|\beta\gamma \nRightarrow \alpha|\beta \quad \vee \quad \alpha|\gamma$$

He gives a *norm* (terme due to **Dirichlet**) to every cyclotomic integer

$$\text{Norm of } f(\zeta) = |f(\zeta)| = f(\zeta)f(\zeta^2) \dots f(\zeta^{p-1})$$

with propriety

$$|f(\zeta) \times g(\zeta)| = |f(\zeta)| \times |g(\zeta)|$$

a cyclotomic number avec de norme égale à 1 est dit *unité*. The task of **Kummer** was the factorization of these numbres[32], un problem considered also by **Jacobi**.

Definition

A cyclotomic number $f(\zeta)$ is *prime*

---

[32] Through his work on cyclootmic numbers, **Kummer** has attracted the attention on the important *field of algebraic numbers*, a subfiled of the field $\mathbb{C}$, that we will see in chapter 3.

$i)$ if $f(\zeta)$ n'est pas une unit

$ii)$ if $f(\zeta)$ divise un product $g(\zeta)\,h(\zeta)$ only one factor .

like **Euler** et **Gauss**, **Kummer** had the new idea by divisibility

Consider the numbers $f(\zeta)$ as integers.

Any prime cyclotomic integer is irreducible but the inverse is not true, there exist des entegers cyclotomic irreducible but not prime !
Comment montrer que $a+b\sqrt{5}$ est irréductible ? on a

Kummer :

Every cyclotomic integer is the product is a prime if

$$|\alpha\,| = |\beta\gamma\,| = |\beta\,|\,|\beta\,|$$

And one of theme is a unit $|\beta\,| = 1$

For example the number $2+i\sqrt{5}$ is irreductible car $\left|2+i\sqrt{5}\,\right| = 21$, but $21 = 7 \times 3$ ce qui donne que $3 \neq$

For the problem of **Fermat** on a when $n = p$ and because the terms $x - \zeta^k y$ are cyclotomic integers

$$x^p \ + \ y^p = (x+y) \ \times (x-\zeta y) \times \ldots \times (x - \zeta^{p-1} y)$$

Kummer discovred that the unicity of factorisation des nombre cyclotomic tombe en défaut when $p = 23$. The problem was how to factorize the numbers $x - \zeta^k y$ where $(x, y) = 1$.
Then to save the unicity of factorization of cyclotomic integers, **Kummer** introduced *ideal complex nombres* (named also *ideal prime divisors* or *ideal factors*). To give an illustration of this problem on donne un exemple :

Example:

the number 6, autre la factorisation triviale : $6 = \pm 1 \times \pm 6$, may be factorised in two if we introduce complex nnumbers

$$6 = 2 \times 3 = (1 + i\sqrt{5}) \times (1 - i\sqrt{5})$$

La première factorisation est dans $\mathbb{Z}$ and the second est dans $\mathbb{C} \supset \mathbb{Z}$(La factorisation *change si on change l'ensemble où on travaille*.) Les quatre nombres 2, 3 et $1 \pm i\sqrt{5}$ sont *non décomposables* dans l'ensemble des nombres $a + bi\sqrt{5}$.

The numbre $3 + i\sqrt{2}$ is an *integer*, we say that it is a *unity* s'il existe un number diviseur égale à 1.

Kummer alors introduced ideal *numbers*

$$\sqrt{2}\ ,\ \frac{1+i\sqrt{5}}{\sqrt{2}}\quad ,\ \frac{1-i\sqrt{5}}{\sqrt{2}}$$

wich means

$$6 = 2 \times 3 = \sqrt{2} \times \frac{1+i\sqrt{5}}{\sqrt{2}} \times \sqrt{2} \times \frac{1-i\sqrt{5}}{\sqrt{2}}$$

An cyclotomic a ideal number

In this new theory, the new prime numbers ou une *generalisation* de nombre premier usuels, $1 - i\sqrt{5}$ est dit un prime. But est-ce que vraiment on ne peut pas factoriser le nombre $1 - i\sqrt{5}$?

Kummer gave the result

Kummer(1840) :

every cyclotmic integer is the unique product of prime ideal numbers.

Kummer introduced *regular prime numbers*. Un nombre premier p est dit *regular* if it verifies

Kummer :

a prime $p > 2$ est *régulier* s'il ne divise pas les numérateurs of **Bernoulli** numbers

$$B_2, B_4, \ldots, B_{p-3}$$

He showed that the following primes less than 164 are irregular[33]

$$37, \quad 59, \quad 67, \quad 101, \quad 103, \quad 131, \quad 149, \quad 157$$

Kummer could then enonciate his great result :

Kummer(1840)

Let $p > 2$ be a prime number , if p is *regular* then the FLT is true for p.

The first irregular prime is 37 , for it divides the **Bernouli** number B_{32}. **Kummer** could not prove that there existe infinité de premiers régulier primes. It has been proved that exist infinity *irregular prime numbers* (**Jensen**

---

[33] It worths to notice that almost all twin primes mentioned are regular

1915). **Kummer** work marqua the importance of algebraic numbers s in the theory of numbers. **Dedekind** will generalize the concept of ideal number to some sets of algebraic numbers called number fields as we will see in later capers.. Tom **Apostol** (19-2015) wrote in 1976 :

> *''Even though Fermat conjecture is still undecided this seems unimportant by comparison to the vast amount of valuable mathematics that has been created as a result of work on this conjecture''.*

Then in 1983 , German mathematician **Faltings** (born in 195) proved

Theorem of **Faltings**

FLT is false for at most finitely integer numbers n.

It was precisely the work of two Japanese mathematicians **Taniyama**(1927-1958) and **Shimura**(19-1) on modular forms which was the key to the problem. Modular forms are functions of complex variable z defined in the upper half plan, their a conjecture known as conjecture of Taniyam Shimura(1857), remaniée afterwards by **Weil**(1967) . **Frey** (1986) discovered a relation with elliptic curves

$$x^2 = y^3 + 1$$

after **Serre** (1987) gave a partial proof of Frey completed at last by **Ribet**(1986) showed that Taniyam-Shimura $\Rightarrow FLT$. Thus he freed the way to **Wiles** to find the of Taniyama-Shimura-Weil conjecture qui fait une entre les modular forms and elliptic curves. We still do not know if FLT implies the existence of infinity many regular primes.

3) Algebraic equations and Galois theory :

Group theory has been initiated by **Galois** (1811-1832) in 1831 after the work of **Lagrange** (1736-1813) on the possibility to find solutions of the polynomial equation

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

en fonction des coefficients $a_0, \dots, a_n$, autrement écrit : trouver les solutions x_n tels que

$$x_n = f_n(a_0, \dots, a_n)$$

Which they call at the time: solve an algebraic equation in *radicals*. Mathematicians have succeeded to find the f_n for $n = 1, 2, 3$ et 4. For example the monome

$$ax + b = 0 \qquad \text{gives} \qquad x = \frac{-b}{a}$$

And also the roots of the quadratic equation $ax^2 + bx + c = 0$ we can write with the use of coefficients[34]

$$ax^2 + (x_1 + x_2)x + x_1 x_2 = 0$$

Also in this domain the roots ζ of unity are involved, they have been considered by **Lagrange**(17-18) and **Vandermonde** (17-18) regarding the solutions of algebraic equations. In his tentatives **Lagrange** he associated to every algebraic equation of degree n, a linear equation called the $resolvante\ t$,

$$t = x_1 + x_2\zeta + x_3\zeta^2 + \cdots + x_n \zeta^{n-1}$$

where $x_1, \dots, x_n$ are the roots of the equation. His method succeeded for $(n = 1,2,3,4)$ for example , for $n = 3$ we have

---

[34] Called *Viète formulas*.

$$t = x_1 + x_2\zeta + x_3\zeta^2$$

where $x_1, \dots, x_1$ are the three roots as before. This implies a relation between coefficients and solution through linear systems.

Afterwards, in 1799 Italian **Ruffini** (1765-1822) proposed a proof of the impossibility of the solutions of any equation of degree five ($n = 5$) in function of its coefficients, a proof completed by **Abel** (1802-1829) in 1829.

Particularly , the two mathematicians showed that the **Lagrange** resolvante does not exist for > 4 , which means qu' on ne peut pas trouver les solutions find f_n such that l'aide known operations

$$+, \qquad -, \qquad \times, \qquad \div, \qquad \sqrt{}$$

Galois has shown that an equation is *resolvable* par radicals if the sets E_1, ..., E_n of coefficients des équations tels que

$$E_1 \subset E_2 \subset \cdots \subset E_{n-1} \subset E_n \dots$$

have some proprieties. Precisely these sets are called *groups* and *fields of* ***Galois***, structures que nous allons étudier later.

Group of substitutions

The first group studied was the group of substitutions of the roots of a polynomial equation by **Galois**.

the finite set of substitutions (special case of transformations) of n éléments is a group called permutations group or *symetric* group $\mathrm{S_n}$, it is also seen as the set of the bijections de S over itself. Permtution of is by a *cycle* or many cycles when abbcca then

$$(a, b, c)$$

If ab and ba but cc we have two cycles

$$(a, b)(c)$$

On définit le produit de deux substitutions of three elements:

$$(c, b, a)(a, c, b) = (c, a, b)$$

The number of elements of this group is $n!$, for example, in the case of three elements a, b and c, the symmetric group[35] is

$$\mathrm{S}_3 = \{(a, b, c)(a, c, b)(b, a, c)(b, c, a), (c, b, a)(c, a, b)\}$$

Inside the ris groups they called sub groups, among thme the alterned subgroup A_3.

Example:

the substitutions group for $n = 4$ qui a des sous-groupes :

− l'ensemble fini $(n = 3)$ des substitutions (a, b, c, d) noted

$$\mathrm{S}_3 = \{(a, b)(a, b)(a, b)() \dots\}$$

− l'ensemble fini $(n = 3)$ des substitution (a, b, c, d) qui conservent le quatrième sont dit *transpositions* forme un groupe dit groupe *alterné*

$$\mathrm{A}_3 = \{(a, b)(a, b)(a, b)() \dots\}$$

− l'ensemble fini de 2 éléments est un groupe *symétrique* G_n lié au transformations géométriques

− the finite set of n elements is a *Klein group* V_n. it is in geometry for we can consider S_4 as the group of rotations and we have

---

[35] The word group was already coined by **Cauchy**(1815) ,and **Gauss** in his book (1801) considred such structure.

$$G_2 \subset V_4 \subset A_4 \subset S_4$$

The G_2, V_4, A_4 are subgroups of S_4 i.e. each group is inside another group. We will in Galois theory a relation between such groups and fields.

the researches that followed like those Jordan on these group of substitutions , **Holder**, **Sylow**, **Dyck**,…enter in the mathematical which founded an important branch des modern mathematics : *modern algebra*. new mathematcal objects were born : les matrices, les transformations, les nombres hypercomplexes, …groups rings ,fields

to well understand modern algebraic features des numbers theory nous we must study the algebraic structures involved

Exercises

1) determinate the 4^{eme} roots of 1.
1) solve the equation $x^2 + ix + 6 = 0$
1) show that for $k \geq 1$ the solutions of the equations:
i) $x^2 + 2kx + k^2 + 1 = 0$
ii) $x^2 - 2kx + k^2 + 1 = 0$
are **Gauss** integers.
1) show that **Gauss** theorem (FTA) is false in the case of many variables**.**

1) do the division $\frac{x^3+x^3}{x+y}$

1) factorise in $\mathbb{C}$:

$$x^2+iy^2, \quad x^2-iy^2$$

1) factorise in $\mathbb{C}$:

$$x^2+y^2,\ x^4+y^4\ , x^6+y^6$$

1) Leinitz thought x^4+a^4 cannot be factorized in $\mathbb{R}$, show he was wrong.

1) show that the product of two integers of the form x^2+y^2 is of the same form(use numbers of the form $a+ib$).

1) why did **Gauss** study the cyclotomic equation $x^p-1=0$ and not cyclotomic equation $x^n-1=0$?

1) verify the identities

i) $(ac-bd)^2+(ad+bc)^2=(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$ (symmetry).

ii) $(ac-2bd)^2+2(ad+bc)^2=(a^2+2b^2)(c^2+2d^2)$

iii) $(ac-3bd)^2+3(ad+bc)^2=(a^2+3b^2)(c^2+3d^2)$

1) find x, y, z and t in function of a, b, c and d such that

$$(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2)=x^2+y^2+z^2+t^2$$

1) give all x, y and z such that $(x-y)(x+y)=z^2$

1) show that to prove : $x^n+y^n=z^n$ has no solutions, it suffices to prove it when $n=prime$.

1) why one should prove FLT for $n=4$ (even if 4 is a multiple of the prime 2) ,compare with $6=2\times 3$.

1) show that the case $x=y$ is impossible if $x\neq 0$.

1) find the solution in the case $x=y=z$.

1) show that s'il n'existe pas une solution positive solutions of FLT , then it is the same with negative solutions.

1) show that $x+y>z$, means that there is no solution of this form: $x+y=z$.

1) show that : $z+y>x$, $z+x>y$.

1) show that if $x, y, z \geq 0$ then $0\leq x<y<z$.

1) show if that $x^n+y^n=z^n$ then $\frac{z}{\sqrt[n]{2}}<\max(|x|,|y|)$

1) prove that the case: $n=14 \Longrightarrow n=7$. Does : $n=7 \Longrightarrow n=14$?

1) assuming FLT show that :

i(x,y) in $x^n+y^n=1$ cannot be both rational for $n>2$.

ii) the equation $x = \sqrt[p]{y^p + z^p}$ has no integer solutions.

iii) if the Phythagorian triple (x_0, y_0, z_0) is a solution, $({x_0}^2, {y_0}^2, {z_0}^2)$ is not.

1) prove that there is not integer solutions of the form $(1, y, z)$.

1) prove that there is not a positive solution of the form (x^2, y^2, z^2) for $x^2 + y^2 = z^2$

1) show if (x_0, y_0, z_0) is a solution for exponent n , then it is not for the exponent kn $(k \in \mathbb{N})$

1) prove that $x^2 + y^2 = 3$ is impossible for integer x, y .

1) give a n integers solution for the equation $x^2 + y^3 = z^4$

1) is there a solution for the equation $x^k + y^l = z^m$ where k, l and m are diffirent intgers

1) show that the equation $x^n + y^n = z^n$ a une solution rationnelle ssi a une solution entière. Donner two solutions entière pour $n = 2$(Pythagorian triples).

1) show that if the equation $x^p + y^p = z^p$ has an integer solution then there existe an infinity. Could you by this and by Faltings result prove FLT ?

1) show that if the equation: $x^n + y^n = z^n$ has solutions l'un au moins des solutions est paire

1) difference between z and y in $x^n + y^n = z^n$ by binomial theorem

1) show that : $x^n + y^n = z^n$ a une infinité de solutions réels. Are there any complex solutions ?

1) is there complex solutions $a + ib \neq 0$ where a and b are integers? Try $n = 3$.

1) what is a rational integer? a non rational integer?

1) say if the numbers are prime in the field of Gauss integers

$$2 + i3\,,\, 2 + i5$$

1) say if the numbers are prime in the field [√5]

$$2 + i\sqrt{5}\,,\, 2 + i\sqrt{5}$$

1) show that p_n a polynomial with roots $x_1, \dots, x_n$, if $p(0) \neq 0$

$$p_n(x) = p(0) \prod_{k=1}^{n} (x - x_k)$$

1) show that

$$p_n(x) - p(0) = x\prod_{k=1}^{n-1}(x - x_k)$$

1) show that S_3 is a group. Is it **Abelian** ? find 1_G .

1) let S_3 the symetric group of three elements, give all its subgroups.

1) consiser $n = 3$ give : S_3 , V_2 , G_2 et A_3.

1) soit S_3 the set of substitutions de trois lettres a, b et c, give 2 examples of transpositions. (groupe alterne A_3)

Supplementary

1) prove that $x^4 + y^4 = z^4$ has no integer solutions.

1) prove that FLT is equivalent to the equation

$$x^p = (z + 2y) \times (z - 2\zeta y) \times \ldots \times (z - 2^{p-1}\zeta^{p-1}y)$$

1) Show that if $0 < x < y < z$ in FLT then $x > n$ (**Gurenet** 1856).

Chapter 2

Algebraic structures

Abstract algebra (or modern algebra) has been much influenced first by number theory, then by theory algebraic of integers. C'est un sujet très vaste, We content ourselves of structures that are necessary to algebraic number theory, these structures are generally already known to the reader .

1)Groups[36] :

Group theory is an essential part of abstract algebra.

***Definition* :**

we sya that G with a law of composition « $*$ » is a group if:

$-\ \forall\ g_1, g_2 \in$ G : $g_1 * g_2 \in$ G , (« $*$ » is internal).

$-\ \forall\ g_1, g_2\ , g_3 \in$ G : $(\ g_1 * g_2) * g_3 = g_1 * (g_2\ * g_3)$, (« $*$ » is associative).

---

[36] Many mathematiciasn from many natiaons have in the establishing of modern algebra so the Germans at the end of XIX centry and begining of XX centry french mathematiians algbraic geometry and but all the dfition the same subject. Chevallet, reder will find somewhat difretnt definition according to the school.

$-\exists 1_G, \forall\, g \in$ G : $g * 1_G = g$, 1_G is *neutral elemnt* of G
$-\forall\, g \in$ G, $\exists\, g^{-1}$: $g * g^{-1} = 1_G$, g^{-1} is the *inverse* of g.

these are the four 'axioms' of the groip concept, they are independent, which means we cannot have one of them from another. The groupe is noted (G, $*$) or (G, 1_G). the first group to be studied was the group of substitutions solutions d'une équation algébrique, il a été étudié par **Lagrange** et **Cauchy**. **Cauchy** was the first to use the word *group* (1815) then **Galois**(183). **Cayley** (18-1) gave the first modern definition of an abstract group (1854) , and especially **Dyck** (1856-1934) in his article (1882).

Remarks :

i) si le nombre d'éléments de G est finite , G is of finite order, we note this number by $\#\, G$, the notations $|G|$, *Card(G)* are also used. Si G n'est pas fini, il est dit groupe d'ordre infini.
ii) si $g_1 * g_2 = g_2 * g_1$ for every g_1 et g_2 on dit que G est un groupe *commutatif* ou aussi *abélien* , expression due à Jordan en honneur of Abel. It comes from the fact that Abel wrote a condition for algebraic equations

$$f(g(x)) = g(f(x))$$

Abelian structures are easier to study than non-Abelian ones. Remark that associtivity of elements is in the same order , so it is weaker then commutativity.

—in the case of a finit group G , peut le present it with a squarred table called *Cayley table*, if G est Abelian le table is symmetric par apport à la principal diagonal.

Examples:

$-$ ($\mathbb{R}$,+) is an additive group (the law is addition $+$) it is of infinite order.
$-$ ($\mathbb{Z}/n\mathbb{Z}$,+) is additive group, abélien d'ordre fini : $\#\ (\mathbb{Z}/n\mathbb{Z}\,, +) = n$.
$-$ $\mathrm{GL_n}(\mathbb{R})$ est un groupe abélien dit *linear group*, set of squared matrices

$n \times n$ noted M_n.
$-$ $\mathrm{O_n}(\mathbb{R})$ est le groupe orthogonal , c'est le groupe des matrices A orthogonales ($A^{-1} = A^T$).
$-$ the set of squared matrices with coefficients in $\mathbb{R}$ muni with multiplication ($\mathrm{A_n}$,×) is a non-commutative group.
-another important group is the *symetric group* we have seen is the permutation of n elements and his is n!.

Torsion of a groupe G :

Definition :

on dit qu'un élément g ∈ G est $de\ torsion$ ou d'ordre k (ou d'ordre fini) s'il existe un plus petit entier naturel k tel que

$$g^k = 1_G .$$

S'il existe un petit unique k pour tout g alors k est dit exposant de G.

the $torsion$ of a group G is the set of its éléments de torsion. On dit que G est un $groupe\ sans\ torsion$ si sa torsion contains only 1_G.

2) Cyclic groups:

Definition :

let G be a group, we say that G is *monogenic* if there exists a such that

$$\forall\ g \in \mathrm{G} ,\ \exists\ \mathrm{n} : a^n = g .$$

The notation a^n means $a * \ldots * a$, the composition of a, n times. A "*generates*" the elements, so a is the *generator* of G, et on note

$$G = \langle a \rangle$$

On peut citer des groups *monogenic* finite like $(\mathbb{Z}/n\mathbb{Z}\,,+)$[37] and infinite groups *monogène* like $(\mathbb{Z}\,,+)$. The appellation *monogène* is not very exact, for it sous-entend que le generator est unique (mono), tandis exist more than one generator in a group as

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$$

If the G is monogenic finite then it is called *cyclic*, so when the generators of the group are more than one, the appellation *monogenic* is not very exact, for it sous-entend que le generator est unique (mono), tandis exist more than one generator in a group.

Theorem:

Every finite Abelian group G is a direct product of cyclic groups.

this means that G is Abelian then there exist $G_1,\dots, G_n$ such that

$$G = G_1 \oplus \dots \oplus G_n$$

In the case of Z

3) Free groups :

Definition :

Soit G un groupe, on dit que G est un groupe *libre sur S* and we note G_s

---

[37] The symbole $n\mathbb{Z}$ presents the multiples of n , so the $\mathbb{Z}/n\mathbb{Z}$ is divided the set $\mathbb{Z}$ by this relation in subsets.

$$\forall\, g \in \mathrm{G},\ \exists\, s_1, s_2 \in\ S \subset G : g = s_1 s_2.$$

The set S here is like a basis for G, the situation is more interesting if G is abelian. Le group $(\mathbb{Z}, +)$ est un groupe libre car $\forall\, n \in \mathbb{Z} : n = 1n$. The group $(\mathbb{R}, +)$ is free too .

Rank of a group :

2) Sous-groups :
the notion of *sub-group* has been by Galois

Definition :

soit $(G,*)$ un groupe, et soit H un sous ensemble de G, on dit que H est un sous-groupe de G si
$-\ \forall\, g_1 , g_2 \in$ H on a $g_1 * g_2 \in$ H
$-\ \forall\, g \in$ H on a $g^{-1} \in$ H.

if H is a sub-group of G, we note it by $H \preccurlyeq G$, on par example

$$(\mathbb{Q},\times) \preccurlyeq (\mathbb{R},\times)$$

Théorème Cayley(1854) :

Tout groupe G est isomorphe au sous-groupe du groupe symétrique S_n (des substitutions)

Les sous-groupes ont des applications importantes :

Lagrange théorèm:

soit G un groupe fini et H un sous-groupe de G alors l'ordre de H divise l'ordre de G autrement :

$$\frac{\sharp G}{\sharp H} \in \mathbb{N}.$$

Le nombre $\frac{\sharp G}{\sharp H}$ est dit *indice de H dans G* est noté $[G \div H]$. **Lagrange** has not assisté to the création of group theory mais son nom, des propriétés ses des groupes de substitutions des équations algébriques que Galois a développé ensuite.

An example of a classical group is **Klein** group V_4, (V from vier four in German)

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

It is easy to prove that this group is commutative.

1-1) The p −groups :

Definition

Let G un groupe fini, si l'ordre de G est une puissance d'un nombre premier (p^k, $k = 1$) on dit que G est un *p-group*.

Prime numbers ont en algebra a lot of special theorems On a des results qui de quelque sorte donnent inverse du theorem de Lagrange du à Cauchy et Sylow on finite groups

Theorem of **Cauchy** :

soit p un nombre premier qui divise l'ordre du groupe G, alors il existe un

sous-groupe H de G d’ordre p.

Cauchy proved this theorem pour les groups de substitutions. D’une autre façon soit p un nombre premier qui divise l’ordre du groupe s’il existe $g \in$ G avec $g^p = 1_G$. L’élément neutre 1_G is generated by g.

5) Sub-groups of Sylow :

a new theory has been created by Norwegian mathematician Peter Sylow(1832-1918) at the end of XIX century on finite groups, we have the following result

Theorem of Sylow(1872)

let G A group such that $p^k | \# \ G$, then there exists a sus-group H of G such that

$$\# \ H = p^k.$$

Ce théorème is important in the classification des groupes finis on a du to Burnside

Burnside theorem :

S est un sous-groupe si H est un groupe ou

The British **Burnside** (1852-1927) was a pioneer in finite groups theory, he émet en 1902 des conjectures sur les groupes finis, une infirmé par Safarvich (1948) and another variant called *restrited Burnside problem*, it has been proved only in 1990 by Russian **Zelmanov** (born in 1955).

2-2) normal sub-groups:

Definition :

On dit que H est un sous-groupe *normal* d'un groupe G si

$$\forall\, h \in \mathrm{H},\ \forall\, g_1, g_2 \in \mathrm{G} \text{ on a : } g_1 h {g_2}^{-1} \in \mathrm{H}$$

if H is a normal subgroup of G then we write

$$H \trianglelefteq G$$

Ces groupes sont dit aussi sous-groupes *distingué* et aussi *invariant*, car le sous-groupe H est stable par rapport à l'opération $*$ du groupe G.
G and 1_G sont les sous-groupes distingués *triviaux* de G. Si G n'a que des sous-groupes distingués triviaux alors G est dit *groupe simple*. Le groupe alterne A_5 est un groupe simple.

4) linear representation of a group :

Une *représentation linéaire* d'un groupe G est un homomorphisme de groupes défined as

$$\rho : G \longrightarrow GL(V)$$

C'est un moyen d'étudier le groupe G.

3) Groupe quotient :

Soit G un groupe on définit une relation d'équivalence sur G

$$\phi : G \longrightarrow GL(V)$$

On a le résultat suivant :

Theorem :

We have

$$Ker\phi \trianglelefteq G \qquad \text{and} \qquad Im\phi \preccurlyeq G$$

3) Topological group :

Soit G a group if the composition is continuous we say that G is a *topological* group, the group of function is topological.

Group theory s a des utilisations inattendues, Il se trouve que les solutions de l'équation de Pell et les points sur an elliptic curve forment un groupe. Aussi **Birch**- **Swininter**-**Dyer** conjecture

Rank of an abelian group is the order of zeros of a certain homeomorphic function

Applications between groups :

Between two groups on peut define des very useful applications

Definition

On dit qu'une application ϕ de G_1 vers G_2 est un homomorphisme de groupes

$$\begin{aligned} \phi : (G_1,\circ) &\longrightarrow (G_2,*) \\ \phi(g_1 \circ g_2) &\longrightarrow \phi(g_1) * \phi(g_2) \end{aligned}$$

Cet homomorphism est dit aussi *representation* de G_1 dans G_2.

the function $f(x) = logx$ est un homomorphisme des deux groupes $(\mathbb{R}^{+*},\times)$ and $(\mathbb{R}^{+*},+)$, for we have for all $x, y \in \mathbb{R}^{+*}$

$$\begin{aligned} log : (\mathbb{R}^{+*},\times) &\longrightarrow (\mathbb{R}^{+*},+) \\ log(x_1 \times x_2) &\longrightarrow log(x_1) + log(x_2) \end{aligned}$$

Remark:

The word *morphism* is from Greek $\mu o\rho\omega\eta$ which means *form*.homomorphism respects the form of the structure, i.e. the structure of the group. *Morphism* is a synonyme of homomorphism.

If the homomorphism is from G_1 to G_1 , il est dit *endomorphism*. *linearity* est un endomorphism of the group $(\mathbb{R}, +)$

$$\begin{aligned} f :\ (\mathbb{R},+) &\longrightarrow (\mathbb{R},+) \\ f(x_1 + x_2) &\longrightarrow f(x_1) + f(x_2) \end{aligned}$$

Si ϕ est bijectif ont dit que ϕ est un *isomorphisme.* Si ϕ est de G_1 vers G_1 , et il est aussi bijectif alors il est dit *automorphisme*.

Kernel and image :

Pour tout homomorphisme de groupes ϕ on peut définir deux ensembles :

— Le noyau : noté ker qui définit comme

$$Ker(\phi) = \{g \in G_1 : \phi(g) = 1_G\}$$

— L'image : notée Im qui définit as

$$Im(\phi) = \{h \in G_2 : \phi(g) = h\}$$

Le $Ker(\phi)$ et $Im(\phi)$ portent des informations sur ϕ autrement :

-si $ker\phi = \{1_G\}$ alors ϕ est un *monomorphisme*
-si $Im\phi$ = G_2 alors on dit que ϕ est un *épimoprphisme*.
-Si ϕ est à la fois un monomorphisme et un épimorphisme, ϕ dit *isomorphisme*. Un isomorphisme est un homomorphisme bijectif, si G_1 et G_2 sont isomorphes ils ont les mêmes propriétés algébriques si G_1 est un groupe G_2 est aussi un group, … si G_1 est commutatif G_2 is also commutatif…

as **Birkhoff** said:

« …One may even describe abstract algebra as the study of those properties of algebraic systems which are preserved under isomorphism »

Example:

soit l'application

$$\begin{aligned} f: \mathbb{R} &\longrightarrow \mathbb{R} \\ f\,(x) &\longrightarrow\ x^2 \end{aligned}$$

the set is a group for both $+$ and $\times$. we have $f(xy) = f(x)f(y)$, but $f(x+y) =\ x^2 + 2xy\ + y\ \neq x^2 + y^2 = f(x) + f(y)$. Ce qui la application f préserve $\times$ mais ne réserve ne pas $+$.

Speaking of homomorphisms and isomorphisms we introduce an important concept:

1) Group action and cosets :

Nous introduisons ici le concept de action de group sur un ensemble X qui lui aussi peut peut-être un groupe.

Definition

We say that $g \in\ G$ agit à gauche on a subgroup H s'il existe une application :

$$\begin{aligned} G \times H &\longrightarrow\ H \\ *\,(g, h_1) &\longrightarrow\ g * h_1 = h_2 \end{aligned}$$

proprieties are very natural

- ∀ g, g$'$ ∈ G and $\forall h$ ∈ H we have $g * (g' * h) = (g * g') * h$
- ∀ $h \in H$ on a $1_G * h = h$

on dit que H est a *left G-coset* noted GH. By the same manner, we define right *G-coset* noted HG, if G is abelian we have

$$GH = HG$$

We may in place of H any set X and G will *act* on X and we say G action. Cosets and action in number they also iestetal in algebraic topology where

isomorphism between is studied.

Remarks :
-si G agit à gauche (ou à droite) sur X cela n'implique pas nécessairement que G agit à droite (ou à gauche) sur X.
- G agit par translation sur lui-même et tout sous-groupe H agit sur G, dans ce cas l'action « **.** » est la loi de composition de G.

Examples:

we considere the vector space le groupe agit sur les vecteur et l'action est la

Théorème :

si G agit à gauche sur un X alors G admet une représentation dans X.

Théorème :

si un sous-groupe H agit sur G alors toute orbite de G par l'action de H a même puissance que H.

Action libre et effective :
si St_x est $\{1_G\}$ on dit que G agit *librement* sur X, si $\bigcap_1^n St_x$=$\{1_G\}$ alors G agit *effectivement*. Et on a action libre ⇒action effective mais action effective ⇏ action libre.

Théorèm :

l'ensemble $\bigcap_1^n St_x$ est un sous-groupe normal de G.

3) quotient Group :
soit H un group normal d'un groupe G alors nous savons que l'ensemble des orbites droit et gauches sont égaux cet ensemble est noté G/H et on peut ainsi définir un groupe dans la composition de deux orbite définit comme suit :

Theorem
le quotient G/H un sous-groupe de G alors l'ordre de H divise l'ordre de G

4) conjugated Action :

soit H un groupe alors on appelle conjugué de H par apport à élément g de G le sous-ensemble de g $H^g = gHg^{-1} = \{ ghg^{-1} : h \in H\}$, l'action x^g est dite action conjuguée le stabilisateur par l'action conjuguée est dit *centralisateur*.

Theorem :

Si alors le est un sous-groupe de H.

2) Rings:

Comme il est bien connu, la théorie algébrique des nombres a donné une généralisation très féconde du concept de *nombre entier*. C'est précisément la motivation de concept *d'anneau* est de généralise the concept of integer i.e. the set $(\mathbb{Z}, +, \times)$ the most original ring

Definition

let A a set with two de composition laws : « $*$ » et « $\diamond$ » such that :

$i)$ (A, $\diamond$) est un groupe abélien

$ii)$ « $\diamond$ » is associative $\forall\ g_1, g_2$ et $g_3 \in$ G on a

$$g_1 \diamond\ (g_2 \diamond g_{3)} = (g_1 \diamond g_2) \diamond g_3$$

$iii)$« $*$ » is distributive par rapport à « $\diamond$ ».$\forall\ g_1, g_2$ et $g_3 \in$ G

on a $g_1 * (g_2 \diamond g_3)=(g_1 * g_2) \diamond (g_1 * g_2)$,

The $(A,*, \diamond)$ est dit a *ring*. The term « *ring* » was coined by Hilbert(1897), and Dedekind used the word « *domain* ». If the law of composition " $\diamond$ " is continuous, we say that A is a topolgical ring. The ring of is topological

S’il existe un élément $1_G \in$ G $\forall\, g \in$ G tel que $g \diamond 1_G = g$, la deuxième opération a un élément neutre pour A, l’anneau A est dit anneau *unitaire*. a ring then is est un ensemble d’entiers généralised pour l’équation la solution est entier. In the all which follows we are intrested in the case where : « $*$ » $:=$ « $\times$ » et « $\diamond$ » $:=$ « $+$ », as a very known example the ring $(\mathbb{Z}, +, \times)$ which satiesfies the above axioms , we have also in this ring : if $a_1 = a_2$ and $b_1 = b_2$ we have $a_1 + b_1 = a_2 + b_2$ and $a_1 b_1 = a_2 b_2$, and equivantly if $c + a = c + a$ and $ca = ab$ then $a = b$ with $c \neq 0$[38].

Remarks :

i) The operation $(\div)$ is not defined everywhere, for $a \div b$ does not give always an integer, thus we say that a ring est clos pour les opérations $(+)$, $(\times)$ et $(-)$ mais pas pour la division $(\div)$.

ii) the set $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is a ring qui a une unité. Un anneau peut avoir *des diviseurs de zéros* like the set of suared matrices, we have $A \times B = 0$ without having A or B soit nulle. Si l’anneau n’a pas de diviseurs de zéro il est dit *intègre* ou *domaine d’intégrité*. Les anneaux intègres sont de loin les plus importants des anneaux, l’anneau $\mathbb{Z}$ et $\mathbb{Z} + i\mathbb{Z}$ (entiers de Gauss) sont des anneaux intègres.

iii) if the opération $(+)$is not abelian on dit que $(A, +, \times)$ est un anneau *non-commutatif*. Here we will always work with t commutative rings.

Definition

the *caractéristique* of a ring is un entier naturel n tel que

$$1_A{}^n = 0_A \quad \text{or the same:} \quad \underbrace{1_A + \cdots + 1_A}_{n\ times} = 0_A\ .$$

If $n = +\infty$ on dit la caractéristique est *nulle*.

Likewise, we say that the application ϕ de A_1 vers A_2 est un homomorphisme d’anneaux

---

[38] This propriety cannot be deduced from the axioms of a ring. It is not satisfied by the ring of real functions on a given interval. A ring that verifies the propriety is called an *integral* ring as we will see shortly [Birkh].

$$\phi : (A_1, \circ) \qquad \longrightarrow (A_2, *)$$
$$\phi(a_1 \circ a_2) \longrightarrow \ \phi(a_1) * \phi(a_2)$$

Avec $\phi(1_{A_1}) = \ 1_{A_2}$

Ring theory has seen more abstract studies due especially to Emmy Noether et Emile Artin. On va maintenant définir un concept important.

3) Ideals :

An important part of a ring is the concept of *ideal*, one of the most important concepts of modern algebra, introduit par Dedekind en 1871, un autre concept similar était celle de *divisor* due to Kronecker.
the decomposition of **Kummer** est vérifiéed que dans le domaine de nombres dit *cyclotomique entegiers*. L'idée de Dedekind de generalize les numbers idéaux à tous les domains of algebraic numbers comme les number $a + bi\sqrt{3}$ (noté $\mathbb{Z}[i\sqrt{3}]$). Dedekind a identifié le facteur *ideal* avec l'ensemble des numbers qu'il divise. This definition peut être applied pour les entiers cyclotomiques comme suit :
l'idéal est un ensemble d'entiers cyclotomiques :

— ∀ a et b des entiers cylotomics alors $a + b$ est un entier cyclotomique
— soit a et b cyclotomiques alors ab est cyclotomique

Ce qui donne la definition in general : Un idéal $\mathfrak{I}$ est un sous-ensemble d'un anneau A vérifiant

Definition

- ∀ a et b ∈ $\mathfrak{I}$ on a $a + b \in \ \mathfrak{I}$, $\mathfrak{I}$ est un sous-groupe de (A, +)
- ∀a ∈ $\mathfrak{I}$ et ∀b ∈ A alors on a : $a \times b \in \ \mathfrak{I}$

Dedekind said that an ideal $\mathfrak{I}_1$ *divides* $\mathfrak{I}_2$ if $\mathfrak{I}_2 \subset \mathfrak{I}_1$. an ideal $\mathfrak{I}$ of a ring A est called *prime ideal* if its divisors are A and $\mathfrak{I}$. Dire $a|b$ est équivalent à dire $\mathfrak{I}_b \subset \mathfrak{I}_a$, et on dit que $\mathfrak{I}_b$ est un diviseur de $\mathfrak{I}_a$, ou de même $\mathfrak{I}_a$ est multiple $\mathfrak{I}_b$, **Dedekind** identifie la division | with inclusion ⊂ .

Examples:

- every ring is an ideal, it is a trivial ideal.
- l'ensemble $\mathbb{Z}$ est un idéal et aussi multiple de 3 l'idéal 3 $\mathbb{Z}$.

Soit les nombres $a_1,\dots, a_n$ on dit que l'idéal $\mathfrak{I}$ est engendré par $a_1,\dots, a_n$ et on note

$$\mathfrak{I} = \langle a_1, \dots, a_n \rangle$$

Un idéal est dit *principal* s'il est engendré par un seul élément a comme l'idéal $5\mathbb{Z}$ est engendré par 5. L'anneau où tous idéal est principal est dit *anneau principal*.

an ideal is amxialis the biggest proper ideal by inclsion: $\mathfrak{I}$ is maximal for all bpossible ideals $\mathfrak{I}_i$ wee have $\mathfrak{I}_i \subset \mathfrak{I}$

Example:

on le précédent des nombres

$$6 = 2\times 3 = \sqrt{2} \times \frac{1+i\sqrt{5}}{\sqrt{2}} \times \sqrt{2} \times \frac{1-i\sqrt{5}}{\sqrt{2}}$$

$\mathfrak{I} = \langle 2,3,6 \rangle$.

$\mathfrak{I} = \langle a_1, \dots, a_n \rangle \subset \langle 2 \rangle$.

3) Modules over a ring :

On dit qu'une partie M d'un anneau A est un *module* si

$\forall\, a, b \in M$ et $\forall\, c, d \in A$

$-(\mathrm{c} + \mathrm{d})\mathrm{a} = \mathrm{ca} + \mathrm{da}$

$-\mathrm{a}(\mathrm{c} + \mathrm{d}) = \mathrm{ac} + \mathrm{ad}$

$-\mathrm{a}(\mathrm{bc}) = (\mathrm{ab})\mathrm{c}$

$-1\mathrm{a} = \mathrm{a}$

in particular, a ring is un A is a A –module.

4) Fields :

Comme le concept de groupe, le concept de corps trouve son origine dans les travaux d'Abel et Galois sur les équations algébriques. Dedekind fut le premier à donner l'appellation *Körper* (d'où la notation K pour un corps). Il donna a d'une autre définit un corps . Le livre de Steinitz (18-19) la *théorie algébrique des corps* (1910) a les premiers résultats sur les corps.

Definition :

let $(\mathbb{A} *, \diamond)$ be a commutative ring. Then we say that $(\mathbb{A} *, \diamond)$ is a *field* if the set $(\mathbb{A},\diamond)$ is a group.

If the group $(\mathbb{A},\diamond)$ is abelien too, we say that the field is commutative; otherwise it is *division ring*[39] .

A field cannot contain divisors of zeros. The set $\frac{\mathbb{Z}}{m\mathbb{Z}}$ is a ring with diviseurs de zéros , but the ring $\frac{\mathbb{Z}}{p\mathbb{Z}}$ n'a pas de diviseurs de zéro, because it is a field. Dans un corps chaque élément a (sauf 0, l'élément neutre par apport to " $*$ ") , an inverse a^{-1} tel que

$$a * a^{-1} = 1$$

the elements of a field qui sont inversible sont dits *les unités* du corps. Un élément α d'un corps (anneau) est dit *premier* si

$-\alpha$ n'est pas zéro ni une unité

$-$si $\alpha|ab$ alors $\alpha|a$ ou $\alpha|b$

The sets $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,+)$ and $(\mathbb{C},+)$ are commutative fileds. Le problème de Fermat a suscité l'émergence de beaucoup d'anneaux et de corps. Le premier système qui nous n'est pas une propriété non usuelle est la non commutativité de la multiplication est le *quaternion* Hamilton en 1843 (et perhaps avant lui Gauss dans des travaux non publiées). Un quaternion (de quatre 4) est un number de la form

---

[39] In French we say that it is *corps gauche*, other

$$a + bi \ + \ cj + \ dk$$

where $i^{2} = j^{2} = k^{2} = ijk = -1$. Hamilton essaya de généraliser les nombres complexes $a + bi$ from the plan to space of dimension 3 sans succès alors il trouva ces nouveaux nombres.
Alors on voit ces nombre défient ce que nous savons des nombres usuelles. L'ensemble des quaternions constitue a non commutatif field (et un anneau non commutatif) car $ij \neq ji$. But Weierstrass proved

Theorem

the can as a group s the the complex numbers C

Un anneau peur être entendu a un corps comme la même façon $\mathbb{Z}$ est entendu à $\mathbb{Q}$, le résultat est dit *corps des fractions*.(aux fractions usuelles de $\mathbb{Q}$).
On remarque que plus une structure a des propriétés plus elle est riche plus elle est apte à résoudre des problèmes. Ces trois structures principales sont : tout corps est un anneau unitaire intègre et tout anneau contient un groupe abélien.

. On va voir maintenant des structures importantes liées au concept de *fields* .

Vectoriel space:

a structure very ancient

Definition

let E un ensemble et K un corps, on dit que E est un espace vectoriel sur le

corps K si
1) $(E, +)$ est un groupe abélien
2) $\forall\ \alpha$ et $\beta\ \in K\ \forall\ x$ et $y \in E$ on a
$-\ \ (x+y)\alpha = x\alpha + y\alpha$
$-(\alpha+\beta)x = \alpha x + \beta y$
$-\ \ \alpha\ (\ \beta x) = (\ \alpha\beta)x$
$-1 \in K, 1x = x$

every commutative field is un *espace vectoriel* sur lui-même. On sait du cours d'algèbre linéaire que tout espace vectoriel une base. Un module M est de quelque sorte un espace vectoriel sur l'anneau A, mais ne possède pas nécessairement une base. On va voir qu'une extension

Algebra structure:

An *algebra* is a vector space E over a field K where we also define a *multiplication* $\times$ between x and $y \in E$

Definition

let E un ensemble et K un corps, on dit que E est un espace vectoriel sur le corps K si
1) $(E, +)$ est un groupe abélien
2) $\forall\ \alpha$ et $\beta\ \in K\ \forall\ x$ et $y \in E$ on a
$-\ \ (x+y)\alpha = x\alpha + y\alpha$
$-(\alpha+\beta)x = \alpha x + \beta y$
$-\ \ \alpha\ (\ \beta x) = (\ \alpha\beta)x$
$-1 \in K, 1x = x$
$-x, y \in E, xy = x$

Mathematisians give here a lot of example of algebras : The sets $\mathbb{R}$ and $\mathbb{C}$ are commutative algebras, the set of analytic (holomorphic) functions forms an algebra.. also the important *Banach algebras* in functional analysis. The first non-commutative algebra et qui a stimulated the study of algebras, est the set of quaternions du to Hamilton in 1843, the result of Frobenius () in 18

Theorem of Frobnius

The algebra of quaternions is the only

De tout ce qui a précédé, le concept de *loi de composition* was capital, mathematicians ont donné libre cours à leur imagination et ont forgé de nouvelles lois de composition que les classiques connus $+, -, \times, \div$, ... pour trouver des nouveaux ensembles avec des propriétés bien différentes. Comme un exemple nous définissons sur $\mathbb{R}^+$ l'opération interne $*$

$$a * b = \frac{1}{2}(|a+b| + |a-b|)$$

Alors on trouve le résultat bizarre $a * a = a$.

Exercises

1) Determinate if the laws $v_1 . v_2$ et $v_1 \times v_2$ are internes on the set of vectors V_n .
1) determine if the two laws $v_1 . v_2$ and $v_1 \times v_2$ are associative.
1) déterminer si la loi $a * b = a^b$ is commutative, is it associative
1) determine if the law " $-$ " is associative in $\mathbb{R}$.
1) determine if law " $\div$ " is associative in $\mathbb{R}$
1) is the law $a°b = \frac{a+b}{2}$ assosiative in $\mathbb{R}$.
1) strangely, the operation " $\times$ " is associative in M_n but not commutative, give two matrices that do not commute.
1) show that : $(ab)^{-1} = b^{-1}a^{-1}$
1) est ce qu'un groupe peut avoir des diviseurs de zéros ?
1) montrer que l'élément neutre 0 n'est pas régulier dans $\mathbb{C}$

1) montrer que l'élément neutre d'un groupe est unique

1) montrer que $a \in (G,*)$ alors $\exists b, c \in G$ tels que $a = b * c$

1) soit $(G,*)$ un groupe, donner ${1_G}^{-1}$

1) soit $(G,*)$ un groupe, montrer que $\forall a \in G, a1_G = 1_G a$

1) soit $(G,*)$ un groupe, montrer que $\forall a \in G, aa^{-1} = a^{-1}a$

1) show that if a^{-1} exists the a is regular. Is the converse true ?

1) how can you show that $\emptyset$ could not be a group?

1) show that the following sets are groups : $(\mathbb{Q}, +)$, $(\mathbb{R}^*,\times)$. Why $\mathbb{R}^*$ and not $\mathbb{R}$?

1) G is a group with $x^2 = e$, show that G is abelian (as **Klein** group).

1) whata re the laws of composition which we defin on the following sets to be groups :

i) $G = \{0\}$

ii) $G = \{1\}$

iii) $G = \{1, -1\}$

1) let $a * b = \frac{1}{2}(a + b + |a - b|)$ montrer que $(\mathbb{R},*)$ is an abelian group

1) let the set $(\mathbb{N},*)$, where $a * b = a^2 + b^2$, is $(\mathbb{N},*)$ a group ?

1) show that : $G = (\{1, -1\},\times)$ is an abelian cyclic groupe.

1) show that : $G = (\{1, -1, i, -i\},\times)$ est un groupe abélien, est ce qu'il est cyclique ?.

1) Let φ a homomorphism of groups G and G' , show that : $\varphi(1_G) = 1_{G'}$

1) montrer que tout groupe cyclique est abélien

1) montrer qui si $x = g.y$ alors il existe un g' tel que $y = g'.x$

1) montrer que l'ensemble des 3eme racines de l'unité $\{1, -\frac{1}{2} + \frac{i}{2}\sqrt{3}, -\frac{1}{2} - \frac{i}{2}\sqrt{3}\}$ muni de la loi $\times$ est un groupe abélien. Généraliser for any n.

1) show that $(\mathbb{Z}/4\mathbb{Z},+)$ is a group.

1) is $(\mathbb{Z}/4\mathbb{Z},\times)$ a group?

1) give the **Cayley** table des group : $(\mathbb{Z}/3\mathbb{Z},+)$.

1) define an equivalence relation $\sim$ in $\mathbb{Z}$. Give all equivalent classes of the $\mathbb{Z}/5\mathbb{Z}$, define the canonical interjection

$$i : \mathbb{Z} \longrightarrow (\mathbb{Z}/3\mathbb{Z} \sim)$$

why it is called so?

1) show that if $H \preccurlyeq G$ then $1_G \in H$

1) montre que si $H \preccurlyeq G$ alors $\forall$ a, b $\in$ H alors $ab^{-1} \in$H.

1) montre que G et 1_G sont des sous-groupes distingués de G .

1) on définit *stabilisateur* de G l'ensemble $St_x = \{ g \in G : g * x = x\}$. montrer que le stabilisateur St_x est un sous-groupe de G.

1) on définit le centre d'un groupe G : $Z(G) = \{g \in G, \forall\, g' \in G: g'g = gg'\}$, montrer que $Z(G)$ est un sous-groupe de G.

1) montrer que si G est abelian then $Z(G) = G$.

1) déterminer tous les sous-groupes d'un groupe d'ordre un nombre premier p.

1) montrer que l'intersection de 2 sous-groupes d'un groupe G est un sous-groupe

1) montrer que $(\mathbb{Z},+,\times)$ is a unitary ring.

1) let $(\mathbb{A},+,\times)$ a commutative groupe,show that $(a+b)c = ac + bc$

1) montrer que l'ensemble des multiples de 3 est un sous anneau de $\mathbb{Z}$, est-il unitaire ? montrer que c'est un idéal, Est-il principal ?

1) montrer que l'ensemble des entiers paires $(2\mathbb{N},+,\times)$ is unitary ring. how about $(2\mathbb{N}+1,+,\times)$ of odd nombres ?

1) soit $(\mathcal{R},+,*)$ un anneau non commutatif, tel que $x * y = xy - yx$

$-$montrer que $*$ est distributive par apport à $+$

$-$monter que $x * y = -y * x$

1) show that the ring $(\frac{\mathbb{Z}}{6\mathbb{Z}},+,\times)$ has zero divisors

1) donner les idéaux de $\mathbb{Z}$

1) montrer que si A is not an integral domain then

$$ab = ac \nRightarrow b = c$$

(is not regular).

1) let $\mathcal{R}$ be a ring, show that : $0_A.a = a.0_A = 0_A$

1) let $\mathcal{R}$ be integral domain , show that the solutions of the equation $xx = x$ are only 0 and 1.

1) let $\mathfrak{I}_1$ and $\mathfrak{I}_2$ two ideals of an integral domain, show that $A \cap B$ is an ideal qui n'est jamais vide.

1) show that a field cannot have zero divisors.

1) show that in a filed we have always :

-if $a_1 = a_2$ and $b_1 = b_2$ we have $a_1 + b_1 = a_2 + b_2$ and $a_1 b_1 = a_2 b_2$

- if $c + a = c + a$ and $ca = ab$ then $a = b$ with $c \neq 0$.

1) is the set of transcendants numbers constitute a field ?

1) let $(\mathbb{R}^{+*}, o, *)$ with $xoy := x \times y$ and $\alpha * y := x^{\alpha}$. show that $\mathbb{R}^{+*}$ is a vector space over $\mathbb{R}$. what is its identity , inverse element .

1) explain why $(\mathbb{Z}/5\mathbb{Z},+,\times)$ is a field.

1) montrer que dans un espace vectoriel élément neutre for × is unique.

- montrer que si $\alpha x = \beta x$ et $x \neq 0$ alors $\alpha = \beta$

- montrer que si $\alpha x = \alpha y$ et$\alpha \neq 0$ alors $x = y$

1) show that if the identity 1 is in an ideal then it the ideal equal to the ring itself

1) show that show that the only proper in a field is {0}.

Suplementary

1) déterminer the law (a, b) is associative

1) prove that if " $*$ " is associative, then x^{-1} exists.

1) soit A un anneau tel que $\forall x \in A :\ x^2 = x$

−montrer que $\forall x \in A : x + x = 0$

−montrer que A est commutatif

1) is it true that $\forall n$, ∃ a group G : $|G| = n$

1) montrer que chaque élément de $(\mathbb{Z}/n\mathbb{Z}$) est inversible que si n est premier

Chapter 3

Theory of algebraic numbers

The problem was: can we theorem sin the integers $\mathbb{Z}$, for new algebraic numbers? this quest have created a very beautiful theory which is theory of algebraic numbers, that freed the road to the theory of *number fields*. We have typical fields we will study field of algebraic numbers

2) Factoriztion in $\mathbb{Z}$ and irreducibility:

The set on integers has proprieties such as divisibility and factorization and the this factorization is unique up to

$$220 = 2 \times 2 \times 5 \times 11$$

We say irreducible if we cannot or a fraction is irreducible we cannot simplfy it

$$\frac{220}{112} = \frac{110}{56} = \frac{55}{28}$$

So the fraction $\frac{55}{28}$ irreducible whereas $\frac{220}{112}$ is reducible. But when we other sets of number look like $\mathbb{Z}$ we diferent that wha has discovred of the XIX century.

And to factorization as **Kummer** that the has the

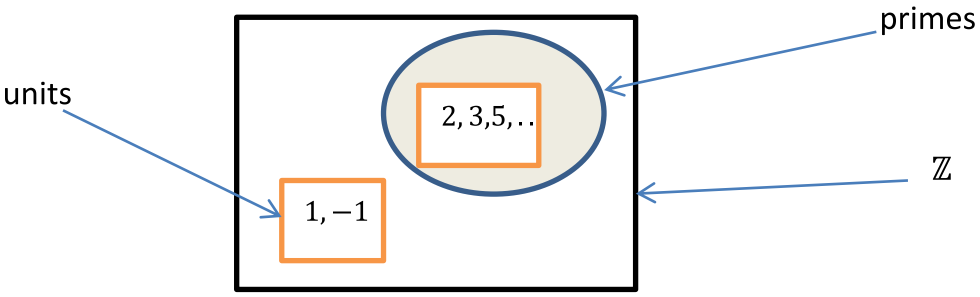


Fig. the set $\mathbb{Z}$. n is prime ⟺n is irreducible

2) Field of algebraic numbers:

The word *algebraic* is intimately linked to polynomial. **Gauss** proved, as we have seen, in 1798 that the algebraic(or polynomial) equation

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

has exactly n roots $a_0, \dots, a_n$ which can be complex numbers $a + ib$.

if the coefficients $a_0, \dots, a_n$ are in $\mathbb{Q}$ (or the same in $\mathbb{Z}$) then the solutions are special, they are the algebraic numbers. L’ensemble des nombres algébriques est un sous-corps de $\mathbb{C}$, car par exemple les nombres $\pi, e, \dots$ are not algebraic. Cyclotomic integers are also algebraic numbers we have seen

$$a_n \zeta^n + a_{n-1}\zeta^{n-1} + \cdots + a_0$$

two sets

i) the set $\mathbb{Q}(\zeta)$ where the coefficients a_n are rationnal is a field called *cyclotomic field.*

Definition
When is 1 and it is a ring only

i) the set $\mathbb{Z}(\zeta)$ where the coefficients a_n are integers is a ring called *cyclotomic ring.*

The field of *algebraic numbers* was the first well studied field, and established the concept of *field* . After the work of mathematicians such as **Kronecker**, **Hilbert**
its is very linked to the theory of factorization and. theory of algebraic numbers are very fascinating

then he foundation of the teory of number fields, we here the to the 206 subsequent chapters.

And the problem that $\mathbb{C}$ is a very special field and algebraic.

Algebraically closed field:

a very important

Examples :

The field $(\mathbb{R}, +,\times)$ is an extension of the field $(\mathbb{Q}, +,\times)$

the notion of *extension* comes from of the theory polynomial equations. Si on a le polynomial

$$x^2 + 2x - 1 = 0$$

dont les coefficient appartient à $\mathbb{Q}$, mais les solution sont $-2+\sqrt{6}$ qui ne sont pas rationnels, l'équation n'est pas réductible sur $\mathbb{Q}$, alors on construit un nouvel corps qui est $\mathbb{Q}+\mathbb{Q}\sqrt{5}$. De même on a le polynomial

$$x^2+2x+1=0$$

Dont les coefficients appartient à $\mathbb{Q}$, mais les solution sont $1+i\sqrt{5}$ qui ne sont pas des rationnels, then we construct a new field which is $\mathbb{Q}+\mathbb{Q}i\sqrt{5}$, alors les deux corps sont des extension de corps $\mathbb{Q}$. Mais lorsque les coefficients sont dans $\mathbb{C}$ like

$$(i+1)x^2+2ix+1=0$$

les solutions sont aussi dans $\mathbb{C}$, ce qui se traduit par : $\mathbb{C}$ est un corps clos algébriquely close, every équation à coefficients dans $\mathbb{C}$ est réductible sur $\mathbb{C}$.

Theorem

The set $\mathbb{C}$ is algebraically close.

this means that any polynomial equations with complex coefficients has its root in $\mathbb{C}$ i.e. the solution are still complex numbers from $\mathbb{C}$, that means we will not discover another new set of numbers.

Exercises

1) show that the solutions of the following equations are algebraic numbers

$\sqrt{2}x - 1 = 0$
$\sqrt{2}x^2 - \sqrt{3}x - 1 = 0$

1) show that the following are algebraic numbers

i) $3\sqrt{2} - 2\sqrt{3}$
ii) $1 - \sqrt{2} - 2\sqrt{3}$
ii) $\sqrt[4]{2} - 2\sqrt{5}$
i) $3\sqrt[7]{\sqrt{2}} - 2\sqrt[5]{\sqrt{3}}$

1) show that the set of numbers (integers) $a + b\sqrt{-n}$ is closed for the three operations

$$+, \qquad -, \ \ and \quad \times$$

what about ÷ ? what do you infer ?

1) prove that a **Gaussian** integer is a quadratic integer.

1) can we apply unicity of factorization to the field of the quaternions?

1) what are the units of the ring $(\mathbb{Z}, +, \times)$?

Chapter 3

Factorial rings

Rings are the central theme of algebraic numbers theory. As the concept of ring is generalization of the set $(\mathbb{Z}, +, \times)$, we will try in the new rings of objects(new numbers, polynmials,..) to study what we have consider in $\mathbb{Z}$: divisibility, unicity of factorisation, **Bachet** theorem, algorithm of **Euclid**,… we will see many examples of rings, et rencontrer beaucoup de problems. First a ring is different from a field, it has no for all element but every field contains a ring.

Factorial rings have been a great tairrin of research. A ring $\mathbb{A}$ is called *factorial* when the factorization[40] of its elements en irreducible factors est unique. We will see that the propriété of unicité of factorization a pu être prolonger à des ensembles comme $\mathbb{Z}[i]$ et $\mathbb{Z}[\xi]$ qui n'ont pas toutes les propriétés de $\mathbb{Z}$.

Definition

---

[40] We can also speak of *factorisation in a field* like in the previous chapter, but since the concept of ring is more genral then a field(every field is a ring) it is more informative to study factorization in rings.

A ring $\mathbb{A}$ is *factorial* if the factorsation of its elements is unique

The first studie factorial ring was of course $(\mathbb{Z}, +, \times)$ et on a dans un anneau des concepts essentiels :

Unities in a ring :

Definition

let A a ring, we say that an élément $a \in A$, est une unité dans A si $a|1$

Pour l'anneau $(\mathbb{Z}, +, \times)$ les unités sont -1 et $+1$. Alors on a ce result.

Factorization

Factorization in $\mathbb{Z}$ has been studied before and numbers that from polynomials , algebraic, are to generalize factorization we can write

$$1 + i|2 + i3$$

But for no algebraic, no polynomial , this has no sens for example

$$\pi|\sqrt{2}\pi$$

This transcendental numbers are not a field.

If have that

$$\alpha|1$$

Then α is called a *unit,* we have

Definition

An algebraic number is prime if on of them is a unit.

Gauss' proof

We have seen that through his work on reciprocity laws , **Gauss** has proved unicity of factorization for two
i) the numbers $a + bi$ called Gaussian integers.
ii) the numbers $a + b\zeta$ where ζ is the third root of 1 .

Principal ideals

The we have result

Theorem

if every ideal $\mathfrak{I}$ is principal , the 'unicity de factorization is always verified otherwise

All ideals are principal ⟺ factorization is unique

Theorem:

let $\mathbb{A}$ be an integral ring, alors l'ensemble des unités de A est an abelian group.

Pour l'anneau $(\mathbb{Z}, +, \times)$ l'ensemble des unités $\{-1, +1\}$ est un groupe abélien pour l'opération × . Alors on a ce résultat

Theorem :

Every principal ring is factorial

$$A\ is\ principal \Longrightarrow A\ is\ factoriel$$

The inverse is false for example A est factoriel mais pas principal.

Samuel could write on **Fermat** in 197 p. 20 :

‘ The opinion aujourd’hui la plus courante est que, dans sa « démonstration », Fermat avait commis une erreur digne de ce mathematicien de premier ordre. Par exemple il aurait pu avoir l’idée (géniale pour son époque) d’opérer dans l’anneau des entiers du corps des racines n-ièmes de l’unité, et avoir cru que cet anneau est toujours principal. En effet on sait démontrer l’assertion de Fermat pour tout exposant n tel que cet anneau soit principal ; mais il ne l’est pas pour tout n ; bien plus, pour n premier, cet anneau n’est principal que pour un nombre fini de valeurs de c'est-à-dire

Remarkable rings :

Quadratic ring :

noted $\mathbb{Z} + \mathbb{Z}\sqrt{m}$, il est dit quadratique car $\sqrt{m}$ est la solution de l’équation quadratique $x^2 - m = 0$.

Ring of cyclotomic integers :

sont les entiers de

Gauss ring :

Noted $\mathbb{Z} + i\,\mathbb{Z}$ or $\mathbb{Z}\,[i]$, its éléments are the Gauss integers, nombres de la forme

$$a + \ ib$$

oue a et b∈ $\mathbb{Z}$. il faut les distinguer des entiers rationnels qui est l’ensemble $\mathbb{Z}$. Gauss avait introduit quand il attaqua la loi de réciprocité biquadratique (n=4) . C’est un anneau d’unique factorisation. Soit α, β et $\gamma \in \mathbb{Z}\,[i]$ On dit que $\alpha|\beta$ s’il existe γ tel que $\beta = \alpha\gamma$. Par exemple $1 + 2i|5$ car $5 = (1 + 2i)(1 - 2i)$. Si un nombre α divise tout entier de Gauss il est dit *unité* de $\mathbb{Z}\,[i]$. Dans cet anneau premier est équivalent à indécomposable. Par la norme N(a+ib) on a un isomorphisme entre $\mathbb{Z}\,[i]$ et R.

Eisenstein ring :

Eisenstein studied reciprocity law for $n = 3$. He introduced his ring noted : $\mathbb{Z} + \omega\mathbb{Z}$, where ω est les 3 racines de l'unité 1. C'est un anneau d'unique factorisation

Anneau de Noether :

Noether has been influenced by Dedekind, his article *théorie idéaux dans les anneaux*(1921). Ces anneaux sont très importants dans la théorie algébrique des nombres. On a $\mathbb{Z}$ est un anneau de Noether. Hilbert a montré que l'anneau des polynômes $K(x_1,\dots, x_n)$ est anneau nothérien.

Anneau de Dedekind :
Un anneau A es de Dedekind si
– s'il est commutatif, unitaire et intègre
– s'il est noethérien
– tout idéal premier non nul est maximal

Les anneaux euclidiens :

On dit d'un anneau euclidien s'il admet l'algorithme d'Euclid.

Theorem :

Tout anneau euclidien est principal ce qui implique qu'il est factoriel.

$$A \text{ is Euclidian} \Longrightarrow A \text{ is principal} \Longrightarrow A \text{ is factorial}$$

efforst by mathematiciens like **Cauchy** to find an algorithm like the Euclid pour les nombres cyclotomiques. $\mathbb{Z}$ est un anneau euclidien. Il est difficile de montrer qu'un anneau est euclidien, par exemple on a cru pour longtemps que le corps quadratique $\mathbb{Q}[\sqrt{97}]$ était euclidien jusqu'à E. Barnes et H. Swinter-Dyer démontra sa fausseté (1952).

other examples of a ring where the unicity of factorization is fasle :

i) the ring $\mathbb{Z}[i\sqrt{5}]$

We have : every prime is irreducible but not every irreducible is prime

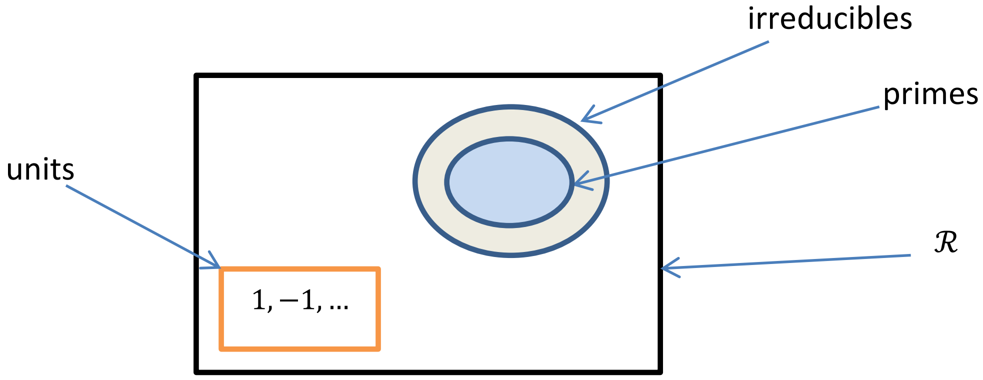


Fig. in a ring $\mathcal{R}$: a is irreducible $\nRightarrow$ a is prime

Exercises

1) what is the dference between integral domain , commutative domain, unitary ring

1) show that the ring $\mathbb{Q} + \mathbb{Q}\sqrt{3}$ has no divisors of zero.

5) show that the numbers 2, 3 and $1 \pm i\sqrt{5}$ are not decomposable in $\mathbb{Q}(\sqrt{5})$.

5) can we factorize $1 + i$ in $\mathbb{Q}(i)$?

1) can we factorize 3 dans $\mathbb{Z}(\omega)$? Dans $\mathbb{Z}(\sqrt{2})$?

1) can we factoriser 2 dans $\mathbb{Z}(i)$?

Chapter 4

Polynomial ring

On va maintenant examiner un anneau très spécial qui a été étudié beaucoup par les mathématiciens du XIX siècle.

The ring of polynomials

We note by $\boldsymbol{E}[\boldsymbol{X}]$, the set of polynômial avec des coefficients in $\boldsymbol{E}$, comme $\mathbb{Z}[\boldsymbol{X}]$, $\mathbb{Q}[\boldsymbol{X}]$ ... we say sole an equation in a domain D i.e. find its solutions in this domain. As we have seen, we sya that r is an algbraic number if it is the solution of an polynomial equation

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

the numbers a_n sont entiers (ou rationnels), if the coefficients $a_n . . a_n$ are relatively prime then the polynomial is *primitive*.
If $a_n = 1$ the équation is called *unitary* and its solutions ar named *algebraic*

integers[41] , because in the simplest polynomial equation $ax + b = 0$ with$(a, b) = 1$, the solution x is an integer iff $a = 1$.

In the set $\mathbb{Q}[\boldsymbol{X}]$, we can alwyas rendre un polynôme unitaire, au contraire de $\mathbb{Z}[\boldsymbol{X}]$.

Minimale polynomial :
we say that a polynomial p is minimale pour la racine α si p the smallest degree tel que $p(\alpha) = 0$.

Theorem :

A number α is algebraic *iff* its minimum polynomial over $\mathbb{Q}$ has coefficients sur $\mathbb{Z}$.

Ce résultat can be généralized to other fields.

Irreductibility:
On dit qu'un polynomial est reducible we can *factorise* it, i.e. write it as the product of two or more factors like

$$x^2 - 1 = (x + 1) \times (x - 1)$$

the are integers, otherwise it is *irreductible* like : $\mathrm{x}^2 + 1$. A irréductible polynômial est comme un nombre premier on ne peut pas le décomposer en autre polynômes de degrés plus petits. But this is not very precise we need some other strict

Definition:

We say that a polynomial is reducible over a field $\mathbb{K}$ if

---

[41] a definition introduced by **Dedekind.**

A polynomial is sseen according to the ring where selon l'anneau its *coefficients* are like :

i) $\mathrm{x}^2 - 1$ is réductible sur $\mathbb{Q}$.

ii) on the contrary $x^2 + 5$ est irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{C}$ for
$x^2 + 5 = (x - i\sqrt{5})(x - i\sqrt{5})$.
in the usual set ring $(\mathbb{Z}, +, \times)$

$$n \text{ is prime} \Leftrightarrow i = n \text{ is irreductible}$$

but when nous entrons un peu dans des ensembles nouveaux, nous trouvons que *premier* n'est pas toujours synonyme de *irréductible*

$$prime \implies irreductible \quad but \quad irreductible \nRightarrow prime$$

le nombre $1 + i\sqrt{5}$ divise 2×3 mais ne divise ni 2 ni 3. Par exemple 2 est irréductible car 2$= a \times b$ alors on $a = \pm 1$ ou $b = \pm 1$. On a la définition

Question

One of the big problems that preocuped mathématiciens les mathématiciens est de savoir si on peut factoriser un polynôme donné?.

Par exemple $x^2 + 5$ est irréductible sur $\mathbb{Z}$ and $\mathbb{Q}$ mais réductible sur $\mathbb{C}$ car
$x^2 + 5 = (x - i\sqrt{5})(x - i\sqrt{5})$.
On a le résultat

Gauss lemma(18) :

If the polynomial $p_n(x)$ is ireductible over $\mathbb{Z}$ then it is irreducible over $\mathbb{Q}$.

Puis un résultat plus

Eisenstein theorem(18) :

Let : $p_n(x) = a_0x^n + \cdots + a_n$, polynomial over $\mathbb{Z}$ $a_i \in \mathbb{Z}$, if

i) $p|a_i$
ii) $p \nmid a_n$
iii) $p \nmid a_0$

Then $p_n(x)$ is reductible over $\mathbb{Q}$

the factorisation is unique si tout nombre irréductible est premier. S'il existe un facteur qui est irréductible mais n'est pas premier la factorisation n'est pas unique. La factorisation des polynômes dépend du corps ou de l'anneau.

Comme les polynômes. Ceci est pour les nombre par exemple 7 est irréductible dans $\mathbb{Z}$ car on peut seulement les facteurs ± 7 et ± 1. Mais il est réductible dans un ensemble de nombres qui est $\mathbb{Z} + \mathbb{Z}\sqrt{7}$ noté aussi $\mathbb{Z}[\sqrt{7}]$, nombre comme $1 - \sqrt{7}$. On trouve

$$7 = \sqrt{7} \times \sqrt{7}$$

Alors lorsque on parle de facteur premier et de factorisation il faut prudent et le semble o on parle. Plus exactement selon *l'anneau* dont on y travaille. Ici des anneau où l'unicité de la factorisation est vérifiée on dit que l'anneau est *factoriel*.

Théorèm :

Si A est un anneau factoriel alors A[x] est aussi factoriel.

Bezout theorem:

We have seen in elementary we can now it in rings called rings

Théorèm :

If A is a ring .

Exercises

1) what are the irreducible polynomials over $\mathbb{Z}$, sur $\mathbb{R}$, sur $\mathbb{C}$:

$a)\ 2x^2+x+1$

$b)\ 2x^2+3x+1$

$c)\ 2x^3+2x^2-3x+1$

1) factorize : $x^{2n+1}+1$

1) factorize: x^5+1 et x^3+y^3

1) factorize n si $n=a^2+b^2$ = c^2+d^2

1) factorize the following

$a)\ 2xy+2yx^2+y^2-xy^2$

$b)\ 2y+yx^2+y^2-xy^2$

$c)\ 2xy+2yx^2-xy^2+1$

1) determine if the set of numbers : $a+b\sqrt{7}$ is a factorial ring, est-il un corps ?

7) donner la division **Euclidian** des polynomials suivants

$-x^2+x+1\ sur\ x+1$

$-3x^3-x^2+x+1\ \ sur\ x^2+2$

$-x+x+1\ sur\ x+$

7) dire si ces polynômes sont réductibles sur $\mathbb{Z}$, $\mathbb{Q}$

$a)\ x^2+x+1$

$b)\ 3x^3-x^2+x+1$

$c)\ x+x+1$

7) déterminer le polynôme minimal de $i+\sqrt{2}$

1) factoriser x^2+y^2 dans l’anneau de Gauss

1) montrer que x^2 -1 est réductible sur $\mathbb{Z}$

Chapter 7

Number fields

Certain mathematician considerate that algebraic numbers theory is nothing then study of number fields what are then number fields?. Apres qu'on a étudié les entiers $\mathbb{Z}$, les nombres algébriques, les nombres complexes of the form $a\sqrt{c}+bi\sqrt{d},$ … on va voir des généralisation des ensemble de ces nombres très important named *number field*.

2) Finite fields:

La notion de corps fini est issu mainly from the work of **Galois** , a finite field is usually called a *Galois field*. Galois travailla sur le corps fini(set of its solution) d'une équation algébrique qu'il nommait « *domain of irrationality* ».

Theorem :

Every finite integral domain A is a field.

Preuve :

soient $a_1 \dots a_n$ les éléments de l'anneau A fini et $a_i a_j = a_k$

le on a le result

Theorem :

let K a finite field, then $\exists\ p,$ such that

$$\sharp\ K = p^n$$

vu qu'un corps contient un anneau, la caractéristique d'un corps est toujours nulle ou un number premier p. The number p ici la caractéristique du corps K, un exemple $\mathbb{Z}/\mathbb{Z}p$

Wedderburn-Dickson theorem (1905) :

Tout corps fini est commutatif.

Revenons au concept d'extension d'un corps.

Local and global fields :

Let $(\mathbb{K},*,\diamond)$ a field as defined before If the composition " $\diamond$ " is continous we say that $\mathbb{K}$ is a topolgical field. The field of is topological

On dit qu'un corps K est local s'il est, il est global si on topologique

Field extension

here a

Definition

On dit que le corps K is an extension of L si $K \subset L$ and we write K/L.

K is seen as a vector space over L , la dimension de l'espace vectoriel K est dite le *degré d'extension* du corps et notée $[K : L]$. si la dimension de K est fin l'extension est fin si la dimension est *infini* alors l'extension est dite *fini*.

-Le corps ($\mathbb{C}^*$,×) est une extension de ($\mathbb{R}^*$,×) the degree is 2

-et le corps ($\mathbb{R}^*$,×) est une extension de ($\mathbb{Q}^*$,×).

On peut présenter l'idée impliquée comme suit : Soit K un corps et un polynôme $p_n(x)$ dont les coefficients sont dans K on à un élément ζ et un ensemble M[ζ] avec toutes les combinaisons de avec les éléments de K. ce M est un corps qui est une extension.

Ce qui a fait **Kummer** est une extension de l'anneau pour sauver l'unique factorisation.

Definition

A number field K is a subfield of $\mathbb{C}$. any field K is a finite extension of the field $\mathbb{Q}$.

On adjoint à $\mathbb{Q}$ avec un nombre $fini\ n$ de nombres algébriques $(a_1, \dots, a_n)$ et on trouve $\mathbb{Q}(a_1, \dots, a_n)$. Le degré est la dimension du corps vu comme un espace vectoriel, un corps algébrique peut être soit fini ou infini.

Observation

Let $p_n(x)$ a polynomial of finite degree n, it has n solution . A number field is the union set $\mathbb{Q}$ and of all complex numbers formed by the operation of : $+, -, \times, \div$ about the roots.

Examples :

1) the field $\mathbb{Q}$ is a number field.

1) the field $\mathbb{Q}[\sqrt{2}]$ is a number field. Its degree is 2 all of degree 2 are called quadratic fields.

2) the field $\mathbb{Q}[i]$ is a number field , it is also noted $\mathbb{Q} + i\mathbb{Q}$, appelé corps des rationnels de Gauss.

3) the field $\mathbb{Q}[\sqrt{n}]$ is a number field, noté aussi $\mathbb{Q} + \sqrt{n}\mathbb{Q}$.

4) the cyclotomique field is a number field, qui est une extension cyclotomique du corps $(\mathbb{Q}, +, \times)$, il est noté $\mathbb{Q}[\zeta]$ où ζ est la racine de 1.

Remark:

The two fields $\mathbb{R}$ et $\mathbb{C}$ are not number fields , because they are not denumbrable. Le corps des usual algebraic numbers aussi n'est pas un corps de nombres car l'extension is not finite.
Vu qu'un corps contient un anneau, l'étude des corps algébrique tient son importance de la structure de l'anneau, tout corps algébrique contient un anneau d'entiers algébriques. L'ensemble des entiers algébriques sont comme l'ensemble $\mathbb{Z}$, il est clos pour les opérations : $+, -, \times, \div$. Cette idée trouve son origine dans les travaux de Galois : il rejoint les racines d'une équation algébrique au corps de ses coefficients pour

Classes des idéaux :

tout corps K étant un anneau, contient au moins deux idéaux, Dedekind montra que sont en classes et que le nombre de ces classes sont fini.

books like *théorie du corps des nombre algébrique* de Hilbert(1897) de Steinitz (18-19) *théorie algébrique des corps* (1910).

Un théorème important du à Dirichlet

Théorème des unités :

Le groupe des unités de l'anneau des entiers d'un corps de nombres est isomorphe au

The class number

1)

Thorem

the class number

$$h_k = 1 \Leftrightarrow \mathcal{O}_{\mathbb{K}} \text{ is } PID.$$

the h_k of $\mathbb{Z}$, $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ is 1.

Return to Kummer :

The work of **Kummer** had great influence on the beginning of modern algebra and algebraic number theory. A ring contains ideals which can be classified in classes, the ideal class number is the number of this classes. Further these classes form a group this group is important to know if the factorization is unique in a ring (a field). Then a prime is regular if

$-\,p$ ne divise pas le nombre de classe h du corps cyclotomique $\mathbb{Q}(\zeta)$ où ζ est la p^{eme} racine primitive.

$-\,p$

Norm of

Kummer defined a norm for numbers of like this:

:

Then the norm of is the determinant of the matrix since every linear application in fite de has a matrix.

Cyclotomic fields:

This field is the set of cyclotomic numbers

Dans son Dedekind le theorem important

Theorem of **Dedekind**(1871) :

Every prime ideal in an algebraic field is the product unique of prime ideals

This result est très essential dans les études algébriques come la geometry algébrique. Dans tous ces généralisation : tous corps algébrique de nombres a un anneau d'entiers algébriques. Quand on cherche l'unicité de factorization dans un corps algébrique K on la cherche dans l'anneau $A \subset K$.

Théorème :

Il y a une infinité de corps algébriques pour qui l'unicité de factorisation is false

Un élément a d'un anneau A est une unité s'il a un inverse dans A. Les unités de $\mathbb{Z}$ est l'ensemble $\{-1, +1\}$. Par exemple dans l'anneau A= $\mathbb{Z}[\sqrt{5}]$, le nombre $2+\sqrt{5}$ est une unité car $(2+\sqrt{5})(-2+\ \sqrt{5}) = 1$. Pour bien il faut bien les unités. Si tous les éléments de A sont des unités alors A devient un corps. Une unité dans corps divise 1 et tous les éléments du corps.

Théorème :

L'ensemble des unités est un groupe abélien.

The solution of Pell equation $x^2 + ay^2 = 1$ consiste à trouver les unités dans $\mathbb{Z}[i]$, car elle peut écrite

$$(x + y\sqrt{a})(x - y\sqrt{a}) = 1$$

Si on ne peut pas différencier les premiers des unités on ne peut pas garantir l'unicité de factorisation.

Exercises

1) montrer que le nombre $\sqrt[2]{3} + \sqrt[3]{2}$ est algébriques

1) montrer que nombres suivants sont entiers algébriques

$$\sqrt{15} + 1,\ i + \sqrt{2}\,,,,$$

2) show that $\frac{i}{2}$ is algébric but not an algebraic integer.

2) soit a et b deux entiers non nuls et $a > b$, montrer que $\frac{a^2+b^2}{a^2-b^2} \notin \mathbb{N}$

1) write $(a^2 + b^2) \times (c^2 + d^2)$ comme somme de deux carrées

1) write $(a^2 - 2b^2) \times (c^2 - 2d^2)$ comme somme de deux carrées

1) factoriser a quadratic equation et exprimer ses racines à l'aide des coefficients des monômes

1) donner les racines d'ordre 3 de l'unité 1.

1) calculate the norm of numbers in number fields:

-
-
-

Chapter 4

Galois Theory

Galois found death in 1832. Inspired by the article of **Lagrange**(1771) *Réflexions sur la Résolution Algébrique des Equations,*

Thus the two concept de *group* and *field* ont vu le jour entre les mains de **Galois** , mais aujourd'hui la *theory de **Galois*** is an independent part of modern mathematics.
Galois theory s'est avérée très importante pour la théorie algébrique des nombres. Elle fait une correspondance entre corps et groupes. Le groupe ici c'est le groupe des permutations des racines d'une équation algébrique dit le groupe symétrique S_n. Galois' ideas fut ensuite developed par **Jordan** (1838-1922) dans son livre classique *Théorie des Substitutions*(1870).

Galois Group :

Galois has shown that to every algebraic equation est associate a group, c'est le group des permutations de its roots, Le group dans son cas est le group de substitutions of the n solutions (roots) of a polynomial equation.

Moreover, a polynomial equation est soluble par radicaux *ssi* le group associated est solvable, i.e. a une suite de sous-groups..
Soit G un groupe et G_i des sous-groupes normaux de G such tha

$$G_1 \lhd \cdots \lhd G_n$$

This subgroup is a *Galois group*. Le Galois group de donne associe à f(x)=0 donne des informations sur f(x)=0 : solvabilité Le groupe G est soluble si.

Extension of a field :

La théorie de **Galois** est théorie qui étudie les corps et leurs extensions, on va voir qu'est-ce qu'une extension de corps :

Définition :

let K_1 and K_2 two field , si $K_2 \subset K_1$ then we say that K_1 est une *extension* de K_2.

The field that used by **Galois** was the domain of the roots of an algebraic eqution

Définition :

Let $K_2 \subset K_1$, then the field is *spliting field*.

g

Definition :

On dit qu'un groupe G est *résoluble*(ou *solvable*) si une de suite de groupe abélien si

$$G_1 \lhd G_2 \ldots \lhd G_n \lhd G$$

Une

Galois Extension :

Pour la théorie de **Galois** we have the following ingrédients

a) une équation algébrique $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ = 0 , ayant n racines $x_1, \ldots, x_n$

b) un corps K comportant les coefficients $a_0, \ldots, a_n$

c) the set P of the root permutations l'équation, which is a cyclic group.

d) groupe de Galois associe à K, qui est le sous-groupe de l'ensemble P.

La question est :

Question:

Can we exprime the roots $x_1, \ldots, x_n$ by the coefficients $a_0, \ldots, a_n$.

the answer to this question

Théorèm :

An équation est soluble par radicaux si le groupe de Galois associé à elle est résoluble.

one of the results of **Galois** was that the équation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

n'a pas être résolue par radicaux, un résultat trouvé à l'aide d'une autre méthode par Abel en 1824.

Le concept de sous-groupe est très important dans la **Galois** theory, on va voir ici un exemple.

Theorem :

Every finite abelian group is solvable.

On a le résultat

Theorem of Sylow(1872) :

Let $E(x) = 0$ an algbraic équation and G its galois group with : $\sharp\ G = p^k$ then the equation is soluble par radicaux.

a result

Théorèm of Moore (1893) :

Tout corps commutatif fini est un corps de Galois.

Galois Résolvante :

Lagrange showed that pour les équations de dégrée 2,3 et 4 on peut résoudre par la méthode de *résolvante de Lagrange*. Comme la résolvante de Lagrange Galois écrit sa résolvante d'une autre

L'existence de la résolvante est équivalente à l'existence d'un sous-groupe normal.

After Galois , mathématiciens se rendent compte que le groupe de Galois peut être défini d'une autre façon

Definition :

let K a filed, we call galois group, the groupe of automorphismes over K.

C'est un sous-groupe de permutations des racines d'une équation algébrique $f(x) = 0$.

Le calcul d’un groupe de Galois :

Calculer un groupe de Galois c’est de

Greeks and the rule and compass

The Greeks had at their disposition deux pratique géométrique: une règle graduée whith which we can draw *lines*, and et un compas qui fait des *cercle* alors la question est de

Question:

Can we draw a segment of length π ?

Une autre question lié à notre problème est la ce que est ce qu’on peut construire le nombre $2\sqrt{3}$.

Galois theory solved the problem de constructability par la *rule and compass* de géométrique.

Exercises

1) détermine les racines de equation $x^6 + x^3 - 1 = 0$ by radical

1) any A is roots find the coeffficients of the polynomial in each case:

i) $(x - x_1)(x - x_2) = 0$

ii) $(x - x_1)(x - x_2)(x - x_3) = 0$

ii) $(x - x_1)(x - x_2)(x - x_3)(x - x_4) = 0$

ii) $(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5) = 0$

how if the is not 1?

1) determine what you can draw with une règle gradué et un compas

1) shwo tat evry circle may be considred of perimeter π

Chapter 4

The p–adic Numbers

We will see here an example of a global field. The *p-adics numbers theory* belong to the algebraic trend that boulvresed mathematics in the XIX century. They were introduced by German mathematician Kurt **Hansel** $(1861-1941)$ in the period $1897-1904$, for number theory, it is now considered as extensions of the set $\mathbb{Q}$ from which it took their origin. They have a relation with analysis, abstract algebra and number theory.

Origin:

i) The existence of p-adic numbers is very simply the solution of congruence of the form

$$x \equiv a \; mod \; p^k$$

ii) let n un integer, we can of course write any n as

$$n = \sum_{k=0}^{k=d} a_k \, 10^k$$

Given any prime number p, on essay to write n comme une série entière au de p

$$n = \sum_{k=0}^{k=d} a_k \, p^k$$

Where a_k are , of course we can for n write

$$n = np^0 + 0p^1 + 0p^2 + \cdots$$

Which is not interesting. As primes are of integer, there is an analogy with the known

$$P_n(x) = \sum_{k=0}^{k=d} a_k \, (x-a)^k$$

A correspondence between p and the factors $(x - a)$.

This series

$$n = \sum_{k=0}^{k=d} a_k \, p^k$$

is finite and unique , a_n are well determined integers such that $0 \leq a_n < p$, alors the result is to write le number n in a new representation

$$n = \overline{a_k a_{k-1} \dots a_0}$$

Then we identify the number n a this sequence of numbers a_k from right to left, it is a *p-adic representation* of the integer n.

Examples:

On a example for $p = 3$

$$10 = 0 + 4 \times 3^0 + 2 \times 3^1$$

a example for$p = 7$

$$100 = 2 \times 7^0 + 1 \times 7^1 + 2 \times 7^2$$

is this unic? then our task is to deal with these new numbers which are les numbers p-adiques

Operation on p–adic numbers

Sum

We can also sum two p-numbers the number 14 and 15 written in 3-adic

$$\begin{aligned} &\ \ 231211 \\ &+ 233333 \\ &- - - - - \\ &= 332222 \end{aligned}$$

The definition of p-adic number us surprises: the series may be infinite!

Subtraction

$$\begin{array}{r} 231211 \\ -\ 233333 \\ -\,-\,-\,-\,- \\ =332222 \end{array}$$

Multiplication

$$\begin{array}{r} 231211 \\ \times\ 233333 \\ -\,-\,-\,-\,- \\ =332222 \end{array}$$

Or for rational number $x=\frac{a}{b}$ we have

$$x=p^{a}\,\frac{c}{d}$$

like

$$\frac{10}{3}=\frac{4\times 3^{0}+2\times 3^{1}}{1\times 3}=2\times 3^{1}$$

The p–adic field $\mathbb{Q}_{\boldsymbol{p}}$

Since the p-adic numbers come from rational numbers, we say that is complete to the norm but is not since $e=2+\frac{1}{3!}+\frac{1}{4!}+\cdots$ although it is sum of rational numbers it is not in $\mathbb{Q}$, so $\mathbb{Q}$ has "gaps" in it. We say ***Cauchy*** sequence if every term get nearer to the other,. To complete it we ad number like e, π,… that this set is the *complete* $\mathbb{Q}$ to get $\mathbb{R}$, so $\mathbb{Q}_{\boldsymbol{p}}$ is also a complete of $\mathbb{Q}$ but it a field $\mathbb{Q}_{\boldsymbol{p}}$ that has very different proprieties .

− the field $\mathbb{Q}_p$ is not totally ordered like $\mathbb{R}$, in $\mathbb{R}$, $\mathbb{Q}$ we have

$$x=y\,,\ x>y\ \text{ or }\ x<y$$

Which is not true in a p-adic field.

$-$since $\mathbb{Z} \subset \mathbb{Q}$ on peut aussi define by the same manner p-adic field $\mathbb{Z}_p$.

The two fields $\mathbb{Z}_p$ et $\mathbb{Q}_p$ are not denumerable as $\mathbb{Z}$ et $\mathbb{Q}$, but non denumerable.

Norm evaluation of p–adic number

let n be a padic number then the $v_p(n)$ is

the exponent of the greatest power of p that divides n

Examples:

example for $p = 3$

$$v_p(10) \ = 2$$

in Analysis the p-adic field is seen also as a metric space. The norm of p-adic numbers are issus as the rational numbers, but there is an essential difference

$$|a|_p = \left| \sum_{k=0}^{k=} a_k \ p^k \right|$$

so we van the norm as

Norm :

$$|a|_p = \frac{1}{p^{v_p(x)}}$$

Examples:

On a example pour $p = 3$

$$|a|_p = \frac{1}{2}$$

a metric space.

The distance $|x - y|_p$

$|x - y|_p = 0$

$|x - y|_p \geq 0$

it has been remarked that the field $\mathbb{Q}_p$ does not verify a very useful and naturel propriety in honor of **Archimedes** , it is named since " ***Archimedes*** *propriety ":*

Propriety of **Archimedes** :

$$\forall a, b\ \exists\ c\ tel\ que\ ab > c$$

the field $\mathbb{R}$ is *Archimedean* for

$$\forall x, y \in \mathbb{R}\ \exists n \quad such\ that\ :\ \ nx > y$$

So the norm $|.|_p$ is not *Archimedean*

$$|x - y|_p \leq \max(|x|_p, |y|_p)$$

which is bizarre, is not a triangle.

Ostrowski theorem (1916) :
gg

The p–adic numbers $\mathbb{Q}_p$ and the zeta function

On a une relation avec la théorie des nombres avec la fonction analytique p-adique

$$\zeta_p = \sum a_k p^k$$

The p–adic algebraic

we results on transcendental numbers to p-adic numbers.

Exercises

1) show that the series $n = \sum_{k=0} a_k\, p^k$ is finite.
1) show that is also unique.
1) write the following numbers with base $p = 5$:

12, 66, 410 , 101

1) write $17 + 23 = 40$ write in the base $p = 7$ and compare the result

1) calculate the evaluation the following numbers with base $p = 3$:

12, 66, 410 , 101

1) find the norm the following numbers with base $p = 11$:

12, 66, 410 , 101

1) show that implies triangle inequality.

1) calculate the norm $|9|_5$

Chapter 6

Quadratic forms revisited

We return now, to quadratics forms seen in la elementary numbers theory des, but now with their algebraic aspect. They are her seen as maps

$$q: \mathbb{R}^n \longrightarrow \mathbb{R}$$

The theory of quadratic forms has played a role prépondérant dans le développement de la théorie algébrique des nombres. Ici on va voir le coté algébrique, on choisit les coefficients dans un corps quelconque, soit $\mathbb{R}$, un corps algébrique, ou même corps p-adique.

Par exemple, un premier est régulier s'il ne divise pas le class number de du corps cyclotomic $\mathbb{Q}(\zeta_p)$ where ζ_p is the $p^{\text{ème}}$ root of 1.
Kummer écrit

$$\sum_{n\geq 1} \frac{1}{N(A)} = \prod_{p} (1 - \frac{1}{N(P)})^{-1}$$

ou A est les diviseur de nombre cyclotomiques et P les diviseurs premiers.

They ideas and some results

i) they defined a new concept the class number .

i) a classification of quadratic forms

i) studied equivalent quadratic forms

i) gave the class formula

i) proved that exits infinitly primes in some forms

Class group:

On classe les formes quadratiques en *classe d'équivalences* et on trouve que cet ensemble constitue un groupe dit $groupe\ de\ classes$

Theorem (18)

L'ensemble des classes des formes quadratiques est un groupe abélien.

Dirichlet considéred forms with des D alors, he has classified them in *classes of equivalence*. Pour l'équivalence de deux forms quadratiques q et q' on utilise l'action d'un groupe G.
two quadratic forms sont *equivalents* si

Il travailla avec le symbole de Jacobi. Il trouve une formule dite *formule de nombre de classes* qui présente le nombre des classes par la valeur de la fonction L au point $s = 1$ et il démontra

$$L(1, \chi) = \frac{hlog(\epsilon)}{\sqrt{D}}$$

between 1935-37 **Siegel** made work on quadratic forms around the du 11th problèm posed by **Hilbert**. Il introduisit les méthodes de l'analyse complex.

Coefficients in a field K

We now studied were not known at te time of Lagrange is the of coefficients os a quadratic form in any fields $\mathbb{K}$ of numbers , but why a field not a group or a ring ? the is

i) a group is a poor structure for our studies because has not the second operation need in our manipulation

ii) a ring although has two operation but has some non-desirable priorities like $a * b = 0$ without a or $b = 0$

It was the German mathematician Hass(18-19) student of Kurt Hansel , who by p-adic numbers to get new results in this domain. Here we will speak of a quadratic form *over a field* $\mathbb{K}$ when the coefficients are in $\mathbb{K}$.

Exercises

1) let the folowing quadratic forms
i) $x_1{}^2 + 2x_1y_1 - 9y_1{}^2$
ii) $x^2 - xy + y^2$
iii) $5x^2 - \frac{1}{2}xy + y^2$
déterminer le D according to **Gauss**

1) soit les formes quadratiques suivantes

i) $x^2 - xy + 2y^2$

ii) $3x^2 + xy - y^2$

iii) $x_1{}^2 - x_1y_1 + 3y_1{}^2$

déterminer le D selon Dirichlet

1) tell if the folowing quadratic forms are équivalentes

i) $-x^2 - 2xy + 2y^2$ and $5x^2 - 3xy + y^2$

i) $x^2 - 2xy + y^2$ and $x^2 - 3xy - y^2$

i) $x^2 + xy + y^2$ and $2x^2 + xy + y^2$

i) 2 $x^2 - 2xy + y^2$ and $x^2 + 2xy + 2y^2$

1) give the class formula for the following

i) $2x^2 + 6xy + y^2$

ii) $x^2 - xy - 2y^2$

iii) $x_1{}^2 + x_1y_1 + 3y_1{}^2$

Chapitre 8

Class field theory

Le lecteur avertie voit bien qu'au cours de ces études algébriques, qu'ils ont quitté leurs buts initiaux (la résolution de équation de dégrée 5, la solution de la conjecture de Fermat, la loi quadratique…) pour entreprendre des études abstraites très éloignées des courants anciens ce qui ces recherches c'est *l'abstraction*.

La théorie de corps de classes émergea de la loi classique de réciprocité, elle étudie la relation existant entre un corps $\mathbb{K}$ est son extension galoisienne, d'une autre façon on essaye des informations sur $\mathbb{K}$ a partir du son extension. Le mot *classe* vient.
Cette théorie a vu un grand développement au cours du XX siècle par les problèmes de Hilbert 9 et 11 :

— la de la loi de réciprocité quadratique pour un corps de nombres quelconque

— classement des formes quadratiques

Les mathématiques impliqués sont le japonais Takaji(18-19) , les allemand Artin et Hasse(1-19). La théorie des corps de classes se compose 2 partie :

—le cas abélien où K est abélien

— le cas non abélien où K n'est pas abélien

En XIX siècle une conjecture par Weber, La conjecture de Weber et Hilbert du cas abélien fut démontré par Takaji en 19.

En 1936 Chevalley invented les *idèles,*(from *élément idéal*) qui une avec les idéaux, puis Weil introduit les *adèles* qui sont des idèles additives.

Anneau des adèles :

Definition :

Une adèle est une anneau topologique c'est-à-dire les deux sont continues

Loi de réciprocité d'Artin :

dans des articles datant de 192 193 , Artin a le problème de Hilbert u il a démontré *la loi de réciprocité d'Artin*

$$:\longrightarrow Gal()$$

Fonctions L d'Artin :
Ce fut Dedekind le premier à définir des *fonction zêta* pour un corps algébrique, c'est une série de Dirichlet ou une fonction $L()$ la représentation linéaire d'un groupe.

Artin écrit

$$\sum_{n\geq 1}\frac{1}{K} = \prod_{p}(1-\frac{1}{K})^{-1}$$

Puis Hecke généralisa les fonctions $L()$ et les zeta de Dedekind. Dans le même courant des grands mathématiciens comme Weil ont construit des *corps de* *nombres* et émet une hypothèse de Riemann pour conjecture démontrée par Deligne en 197.

on a

Theorem of Weber-Kronecker :

Every finite abelian extension de $\mathbb{Q}$ corps de cyclotomique.

This theorem was proved, après les tentatives de Kronecker et Weber, par Hilbert en 1896. Kronecker le nomma *'Jugentraum'* (rêve de jeunesse),

Nous avons la loi de réciprocité cette théorie est une sorte de généralisation de la loi.

Gauss a conjecture une par en 19. Puis ont un résultat plus fort.

Exercises

1) montrer que trois racine de l'unité sont 1, ζ et ζ^2
1) soit ζ une n^{eme} racine primitive de 1 montrer que 1+ $\zeta + \cdots + \zeta^{n-1}$ = 0
2) trouver les racine de la forme $ax^2 + bxy + cy^2 = 0$
2) résoudre l'équation $ax^5 + bx^{\frac{5}{2}} + c = 0$
2) trouver le reste de la division du polynôme $x^4 + 2x^2 + x - 1$ sur le polynôme $x + 1$
7) montrer que $\mathbb{R}$ a une infinité de sous-corps
5) on montre que l'ensemble des nombre algébriques est un corps ,montrer que $2i + \pi$ n'est pas algébrique

Open problems

Since open problems in algebraic number theory are linked to abstract algebra, usually they have links with other *algebraic* disciplines like algebraic topology and algebraic geometry.

1) We know since **Jansen**(19) that there are infinitely many irregular primes. Is there infinitely many regular prime numbers?
2) the **Kummer**-**Vandiver** conjecture.
3) What are the factorial domains $\mathbb{Q}[\sqrt{d}]$ when $d > 0$?
4) existe-il une infinité de corps avec unicité de factorization ?
5) reciprocity la for non abelian case.
6) the **Tate** conjecture.
7) the **Leopoldt** conjecture.
8) the **Stark** conjecture.

Third part:

Analytic number theory

Gustave **Lejeune-Dirichlet**

Chapter 1

The orders of infinity

One of the preoccupations of analytic numbers theory is how a function f changes in respect of another function. **Hardy**

> *" The notion of the 'order of greatness' or ' order of smallness' of a function f(n) of a positive integral variable n, when n is' large' ,or of a function f(x) of a continous variable x, when x is large or small or nearly to a , are of the greatest importance even in the most elementary stages of mathetical Analysis."*[42]

1) Infinitely small and infinitely big

We say that a quantity a (which depends of x) i *infinitely small* when $x \longrightarrow x_0$ if

$$\lim_{x \longrightarrow x_0} a(x) = 0$$

---

[42] *Orders of Infinity*, p.1.

By the same, we say that a quantity a is *infinitely big* if

$$\lim_{x \longrightarrow x_0} a(x) = \infty$$

In both cases, x_0 may be also $\pm\infty$.

In many situations, we demand how a quantity is infinitely small or infinitely big, we are interested in the $speed$ of decrease or the *speed of increase* ,we also say rate of increase (or decrease) that we name in general $order\ of\ increment$, order of infinity , scale of infinity. or we like to study

1)if a function f tends to a limit

2) if a function f tends to a limt more or less rapidly than g , we study the

$$\lim_{x \longrightarrow x_0} \frac{f(x)}{g(x)} = \ ?$$

to illustrate this problem we give some real examples and the complex $z\ = x + it$ can be treated by the same method. We usually use in number theory, the limit when $x \longrightarrow +\infty$, but in many occasions we also treat the limit when $x \longrightarrow \pm\infty$ (or simply $x \longrightarrow \infty$) especially in complex variables.

Example 1:

the two functions $\frac{1}{x-1}$ and $\frac{2}{(x-1)^2}$ both infinitely small when $x \longrightarrow\ 1$ but if we compare them

$$\lim_{x \longrightarrow x_0} \frac{\frac{1}{x-1}}{\frac{2}{(x-1)^2}} = 0$$

the functions $\frac{1}{x-1}$ et $\frac{2}{(x-1)^2}$ are not of the same $order\ of\ increment$ when $\longrightarrow\ 1$, precisely the function $\frac{1}{x-1}$ tends 0 more rapidly than the function $\frac{2}{(x-1)^2}$.

Example 2 :

Les sont tous les deux $\frac{1}{x}$ and $\frac{2}{x^2}$ are des infiniment petit lorsque $x \longrightarrow \pm\infty$ but if we compare them

$$\lim_{x \longrightarrow x_0} \frac{\frac{2}{x^2}}{\frac{1}{x}} = 0$$

so the two functions ne sont pas du *même ordre de croissance* lorsque $x \longrightarrow \infty$ .The function $\frac{2}{x^2}$ go to 0 more rapidly than $\frac{1}{x}$.

Another example when we limit of function, the function x and $log\ x$ when $x \longrightarrow 0$, but we have the limit

$$\lim_{x \longrightarrow 0} xlog(x) = 0$$

Which means that x goes to 0 faster than $log\ x$ goes to $-\infty$.

Exemple 3 :

the two functions $\frac{1}{x-1}$ et $\frac{2}{x-1}$ sont tous les deux des infiniment petits lorsque $x \longrightarrow 1$, but if we compare them we find

$$\lim_{x \longrightarrow 1} \frac{\frac{2}{x-1}}{\frac{1}{x-1}} = 2$$

Then the two functions $\frac{1}{x-1}$ and $\frac{2}{x-1}$ are of the *same order ofincrement* when $x \longrightarrow 1$.

Example 4 :

Les sont tous les deux x and $\sin(x)$ are infiniment small lorsque $x \longrightarrow 0$ mais si on les compare entre eux

$$\lim_{x \longrightarrow 0} \frac{\sin(x)}{x} = 1$$

Alors les deux functions sont pas du *same order de croissance* what is more is they are equivalent, also for

$$\lim_{x \longrightarrow \infty} \frac{x-1}{x} = 1$$

we say that they are *equivalents*, also x and $xcox$ are equivalent when $x \longrightarrow 0$

$$\lim_{x \longrightarrow 0} \frac{xcos(x)}{x} = 1$$

Example 5 :
sometimes we cannot make a comparasion between two quantities:

For the two functions $(-1)^n$ and $\sin(n)$

$$\lim_{n \longrightarrow +\infty} \frac{(-1)^n}{\sin(n)} \quad does\ not\ exist$$

also $\cos(x)$ and $\sin(x)$ have no limit when $x \longrightarrow \infty$ and we cannot compare them either

$$\lim_{x \longrightarrow \infty} \frac{\sin(x)}{\cos(x)} \quad does\ not\ exist$$

Observation

There are three exeptional functions in mathematics that are every one is *radically different* from the two other and the reader must know and use later:

i) polynomial: $P_n(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$

ii) $logx$,

iii) exponential a^x , $a > 1$, the very used[43] is e^x

we ha two principale proprieties

Lemma

$$\lim_{x \longrightarrow +\infty} \frac{log^{\alpha}(x)}{P_n(x)} = 0 \qquad and \qquad \lim_{x \longrightarrow +\infty} \frac{P_n(x)}{e^x} = 0$$

These considerations can be practically well written and manipulated by the *notation of Landau*. This notation is useful particularly if we do not know f because it is difficult to manipulate analytically.

2) Notation of Landau :

We findd that mathematicians used inequalities to estimate functions, like Borel used K in like

$$f(x) \leq Kg(x)$$

In practice we use today two symbols " ***O"*** and ***"o"*** known as ***Landau's*** *symbols*, . The symbol " ***O"*** first used by German number theorist **Bachmann**(1837-1920) in his book *Zahlentheorie*[44] (1892-1894) , where Edmaund **Landau**(1877-1938) who first noticed it . Later Landau himself added another symbol "***o"*** in his book "*Handbook of the distribution of prime numbers"* (1909).

---

[43] Notice that x^x is simply e^{xlogx}

[44] In fact, in the 1894 edition p.401, **Bachman** was the first to write: "$\tau(n) = nlogn + O(n)$" , O is the first letter of "*Ordunung*" = order, he meant " *order of n*".

These notations are used when we want to compare two quantities either in the neighborhood of a finite number x_0 or in the neighborhood of $\pm\infty$.

We usually use:

a) ***l'Hopiltal*** *rule*.

$$\lim_{x\longrightarrow 0}\frac{f(x)}{g(x)}=\lim_{x\longrightarrow 0}\frac{f'(x)}{g'(x)}=\cdots$$

b) **Euclidian** theorem for sequences and series

$$\left|\sum u\right|\leq\sum|u|$$

c) **Euclidian** theorem for definite integrals

$$\left|\int f dx\right|\leq\int|f|dx$$

$a)$ Big $\boldsymbol{O}$:

We say that f and g are of the same order of magnitude et we write

$$f=Og(x)$$

if

$$\lim_{x\longrightarrow\infty}\frac{f(x)}{g(x)}=C<\infty$$

or the same if there exist a positive constant C and a real x_0 such that

$$|f(x)|\leq Cg(x)\quad\text{for all } x:\quad x\geq x_0$$

This O is a constant we often do not know its exact value but we are satisfied by its existence and above all, we search for optimizing it.

Observation

If we have

$$f = Og(x)$$

we say that $f \in Og$ or f is Og.

Examples :

1) if $f(x) = n^2 + 2n + 1$ then $f(x) = O(n^2)$ for we can write $n^2 + 2n + 1 < 4(n^2)$, but also more precisely we can write : $n^2 + 2n + 1 < 2(n^2)$. Since $4 > 2$, then $2(n^2)$ is more precise.

2)if $f(x) = 5x^3 + x^2$ then $f(x) = O(x^2)$ for $\lim_{x\longrightarrow 0} \frac{f(x)}{x^2}$ is bounded when $x \longrightarrow 0$ as

$$\lim_{x\longrightarrow 0} \frac{f(x)}{g(x)} < \infty$$

We can also have $f = O(x)$, but $O(x^2)$ is the best approximation , for if $n > 2$:

$$\lim_{x\longrightarrow 0} \frac{f(x)}{x^n} = \infty$$

And therefore for $\varepsilon > 0$: $f \notin Og(x^{2+\varepsilon})$.

as an famous example we trying since 1859 to prove that

$$\int_2^x \frac{dt}{logt} = \frac{x}{logx} + O(x^{\frac{1}{2}+\varepsilon})$$

which is equivalent the Riemann Hypothesis, without success.

Observation:

$$f = O(1)$$

means that f tends to a constant when $x \longrightarrow x_0$.

b) Little "o" :

We say that : $f = og(x)$ if

$$\lim_{x \longrightarrow \infty} \frac{f(x)}{g(x)} = 0$$

Which means that f is very small devant g

Notation

notation

$$f = o(1)$$

means that f tends towards 0 when $x \longrightarrow x_0$

in this context as we have observed, we find three totally different animals in the word of functions

$$e^x, \quad P_n(x)\,, \quad logx$$

Such that

$P_n(x) = o(e^x)$

$log(x) = o(p_n(x))$

$log(x) = o(e^x)$

c) Equivalence:

If f and g very proche i.e

$$\lim_{x \longrightarrow \infty} |f(x) - g(x)| = 0$$

we write

$$f(x) \sim g(x)$$

Wich means

$$\lim_{x \longrightarrow \infty} \frac{f(x)}{g(x)} = 1$$

We say that f is *asymptoic* to g , or verse versa. That can be also written

$$f(x) = g(x) + og(x)$$

Subsequently, we will see a result that took 100 years to be proved namely

$$\pi(x) \sim \int_{2}^{x} \frac{dt}{logt} \sim \frac{x}{logx}$$

We say that f has the same order of magnitude as g , especially this helps us to if f converges if g converges the two operators

$$\int \quad \text{or} \quad \sum$$

They converge (or diverge) at the same time.

If two series such: $u = Ov$

Then $\sum u$ and $\sum v$ converge or same time

If two functions such : $f = Og$

then $\int f$ and $\int g$ converge or diverge at the same time

For the notation o the situation is different.

2) Hardy and Littlewood :

Afterwards, following an article published[45] by German mathematician **Paul Du Dubois-Reymond** (1831-1889) who introduced some notation like

$$\prec, \quad \succ, \quad \gtrless, \quad \sim, \quad \precsim$$

Hardy(1877-1947) in his book “*Orders of Infinity*” (1910) , introduced six more notations

$$\prec\prec, \quad \succ\succ, \quad \asymp, \quad \preccurlyeq, \quad \succcurlyeq, \quad \overline{\asymp}$$

1) We use the notation

$$f \asymp g$$

to mean that there are two constantes c_1 and c_2 such that

$$c_1\, f(x) \leq g(x) \leq c_2\, f(x)$$

In 18 **Chybechev** (18-1) proved that

---

[45] Under the title:" *Uebr die Pradoxen des Infinitärcalculüs*"(" *on the Paradoxes of the infinities calculus*") ,in *Mathematische Annalen*, volume XI (1877), 149-167.

$$\pi(x) \asymp \frac{x}{logx}$$

namely that

$$c_1\,\pi(x) \leq \frac{x}{logx} \leq c_2\,\pi(x)$$

2) if f is very small before g, ou de with our new notation

$$f \prec g$$

Means as we have seen before: $f = og$, or

$$\lim_{x\longrightarrow\infty}\frac{f(x)}{g(x)} = 0$$

and inversely if $\lim_{x\longrightarrow\infty}\frac{g(x)}{f(x)} = 0$, then

$$f \succ g$$

or $g = o(f)$

3) for

$$|f(x)| \leq Cg(x)$$

Hardy wrote

$$f \preccurlyeq g$$

And we may write

$$f = Og \;\;\Leftrightarrow\;\; f \preccurlyeq g$$

Or if

$$f > K_1 g \ , \quad f < K_2 g$$

But since

$$f = Og \ \Longrightarrow \ g = Of$$

or

$$f \preccurlyeq g \ \Longrightarrow \ f \succcurlyeq g$$

then he noted that

$$f \asymp g$$

4)if then $\lim_{x \to x_0,\infty} \frac{f(x)}{g(x)} = 1$

$$f \sim g$$

5) Another notation due to both **Hardy** and **Littlewood** is

$$f = \Omega(\mathrm{g})$$

Means

f is not negligeable if compared to g

In their article of 1914:

"…we shall find it convenient at this stage to introduce a new notation. We define the equation

$$f = \Omega(\varphi)$$

Where is appositive function of a variable, which may be integral or continuous but which tends to a limit, as meaning that there exists a constant H and a sequence of values of the variable, themselves tending to the limit in *question, such that*

$$|f| > H\varphi$$

for each of these values. In other words, $f = \Omega(\varphi)$ *is the negation of* $f = o(\varphi)$*."*[46]

3) Vingradov's notation:

In his of analytic number theory the Russian **Vinogradov**(198-19) his proper notation around 1930s

$$\ll \quad , \quad \gg$$

He certainely knew **Landau** notation, because German language was common in scientific publishing. This difference in notation is not appreciated, it would be better to unify language to simple the work of others, but every nation *(chauvinism oblige*!) loves to invent and use its proper things, especially in Europe and at the Soviet era!

Vinogradov wrote

$$f(x) \ll g(x)$$

or the same

$$g(x) \gg f(x)$$

which is equivalent to

$$f(x) = O\big(g(x)\big)$$

---

[46] "*Some problems of Diophantine approximation*". Acta. 37.

but less than $<$ that g is bigger than f which is the opposite, it is preferable for a notation to be *mnemonic*.

4) Superior and inf limits of a sequence or a function:

Also we meet with two concepts

$$limsup_n(u_n) \quad \text{and} \quad liminf_n(u_n)$$

Noted also

$$\overline{lim}(u_n) \quad \text{and} \quad \underline{lim}(u_n)$$

these limits always exist and are either a finite number a or ∞. They have been introduced when there are problems de limite a sequence u_n n'a pas de limite bien définie.

Example

The two sequences $(-1)^n$ and $\sin(n)$ have no limits but after all

$$limsup_{+\infty}(-1)^n = 1 \quad \text{and} \quad limsup_{+\infty}\sin(n) = 1$$

also

$$liminf_{+\infty}(-1)^n = -1 \quad \text{and} \quad liminf_{+\infty}\sin(n) = -1$$

If u_n has a well defined limit , then we have

$$\underset{+\infty}{liminf}\, u_n = \underset{+\infty}{limsup}\, u_n = +\infty$$

Exercises

1) Determinate the infinitely small and infinitely big when $x \longrightarrow 0$

a) $\frac{x}{logx}$

b) e^{-x}

c) xe^{x}

d) $\frac{sinx}{x}$

e) $\frac{sinx}{cosx}$

f) $\frac{logx}{x}$

g) $\frac{logx}{sinx}$

h) $\frac{logx}{cosx}$

i) $\sqrt{x+1}-\sqrt{x}$

1) Determine the infinitely small and infinitely big when $x \longrightarrow \infty$

a) $\frac{x}{logx}$

b) e^{-2x}

c) $\frac{-x}{logx}$

d) xe^{-x}

e) $x-e^{x}$

f) $x+\sin(x)$

g) $\frac{logx}{sinx}$

h) e^{xlox}

i) e^{-x}

1) determine the infinitely small and infinitely when $x \longrightarrow 0$ and write it with **Landau** notation

a) $\frac{x}{logx}$

b) e^{-x}

c) xe^{x}

g) $\frac{sinx}{x}$

n) $\frac{xcosx}{sinx}$

g) $\frac{logx}{x}$

g) $\sqrt{x+1}-\sqrt{x}$

g) $\frac{\sin(x)}{x}$

h) $\frac{cosx}{xsinx}$

1) Determine the infinitely small and infinitely big when $x \longrightarrow \infty$ and write it with **Landau** notation

a) $\frac{x}{log}$ and x

b) xe^{-x} and x

c) $\sin(x)^{\frac{1}{x}}$ and x

d) e^{-2x} and x

e) e^{x} and x

f) $\log(x)^{\frac{1}{x}}$ and x

g) $\frac{-x}{log}$ and x

h) $n^{\frac{1}{n}}$ and x

i) $e^{\frac{1}{x}}$ and e^{x}

j) kx and x

k) $\sin(x)$ and k

l) x and x^{2}

m) kx and $x + k$ n) $\sin(x)$ and x

1) Compare between every two functions when $x \longrightarrow 0$ and write it with **Landau** notation

a) $\frac{x}{logx}$ and $\frac{\sin(x)}{x}$ b) $\frac{sinx}{x}$ and $\frac{logx}{x}$ c) e^{xlox} and e^{x}

d) e^{-x} and $\frac{logx}{sinx}$ e) $\frac{cosx}{sinx}$ and xe^{x} j) $\sin(x)$ and x

f) kx and x g) $\sin(x)$ and k h) x and x^2

i) kx and $x + k$

1) compare between every two functions big when $x \longrightarrow \infty$ and write it with **Landau** notation

a) $\frac{x}{log}$ and e^{-2x} a) xe^{-x} and e^{x} v) $\sin(x)^{\frac{1}{x}}$

b) $\frac{-x}{log}$ f) $n^{\frac{1}{n}}$ and e^{x} g) $\log(x)^{\frac{1}{x}}$

repeat the exerciec using both **Vingradov** and **Littlewood** notations.

1) suppose that $f = Og$, are the following true

a) $f(x) \leq C|g(x)|$

b) $|f(x)| \leq |Cg(x)|$

c) $|f(x)| \leq cg(x)$

1) suppose that $f = og$, are the following true

a) $\lim_{x \longrightarrow x_0} \frac{f(x)}{|g(x)|} = 0$

b) $\lim_{x \longrightarrow x_0} \frac{|f(x)|}{g(x)} = 0$

c) $\lim_{x \longrightarrow x_0} \frac{|f(x)|}{|g(x)|} = 0$

1) for $\alpha > 0$ find the limit

$$\lim_{n\to+\infty} \frac{x(\, log(x) - \alpha)}{\log^2(x) + \alpha\log(x)}$$

1) show that if f and g are integrable functions on $[0, x]$ and if $f(x) = Og(x)$ then:

a) $\int_a^x |f(t)| dt = O \int_a^x g(t)\, dt$
b) $\int_a^x f(t) dt = O \int_a^x |f(t)|\, dt$

2) let $p_k(x)$ a polynomial of finite degree k , show that if $x \longrightarrow \infty$:

i) $p_k(x) = o(e^x)$
ii) $log^n(x) = o(p_k(x)\ )$
iii) $log(x) = o(x^\alpha) \quad \alpha > 0$

1) show that if $x \longrightarrow 0$:
i) $\log(x) = o(\frac{1}{x})$,
ii) $x^n = o(x^m),\ \ n > m$
1) is it true: $f = Og \ \ and \ \ g = Oh \ \ then \ \ f = Oh$
1) show that if $x \longrightarrow 0$:
$o(x)o(x) = o(x)$

1) show that $O(f + g) = O(g) + O(f)$
1) show that $kO(x) = O(x)$ if $k \neq 0$
1) show that $O(f + f) = O(f)$
1) show that $O(x)O(x) = O(x^2)$
1) show that $\sim$ is commutative
1) show that $kO(x) = O(x)$, if $k \neq 0$
1) show that $ko(x) = o(x)$, if $k \neq 0$
1) show that $ko(f) = o(f)$, if $k \neq 0$
1) show that $f(x) = O(1) \Longrightarrow f(x) = o(x)$
1) show that: $f(x) = og(x) \Longrightarrow f(x) = Og(x)$. (in **Hardy** notation: $f \prec g \Longrightarrow f \preccurlyeq g$)
1) is it true $f(x) = Og(x) \Longrightarrow f(x) = og(x)$
1) montrer que et $f \sim g \iff f = g + o(g) \iff g = f + o(f)$
1) we have seen that : $2^n > n$ and $e^n \geq n + 1$ for $n \geq 0$, write that in **Landau** notation

1) compare between : e^n and 2^n in **Landau** notation

1) show that : $\gamma = \int_1^{+\infty} \frac{\{x\}}{x^2} dx < 1.$

1) find X such that if $x \longrightarrow X$: $log(n+1) - log(n) \sim \frac{1}{n}$

1) find X such that if $x \longrightarrow X$: $\sum_0 e^{-\pi n^2 x} = O(e^{-\pi x})$

1) Show that $\lim_{n\to\infty} n - \sqrt{n} = +\infty$. Write the result in O-notation, then show that the series $\sum_1 \frac{1}{\sqrt{n}} - \frac{1}{n}$ is divergent.

Supplementary exercises

1) show that $o(f+g) = o(g) + o(f)$

1) are « O » and « o » commutative ?

1) show that $O(x)O(x) = o(x)$

1) if $x \longrightarrow 0$: show that $O(x) + O(x) = O(x)$

1) if $x \longrightarrow 0$:show that $o(x) + o(x) = o(x)$

1) give limsup and liminf of the following if $n \longrightarrow \infty$

i) $\frac{(-1)^n \sin(x)}{\cos(nx)}$

iii) $\frac{\sin(x)}{(-1)^n \mathrm{n}\cos(x)}$

iii) $\frac{(-1)\sin(nx)}{\cos(x)}$

iv) $\frac{\mathrm{n}\sin(x)}{(-1)^n \cos(x)}$

Chapter 2

The Work of Dirichlet

Through his tentative to prove quadratic reciprocity law conjectured by **Euler**, the French **Legendre** $(17-18)$ gave a proof that reposed on a mathematical propriety which he took for granted , but not evident, namely that there exists infinity many prime numbers in every (progression) of the form $ak+b$ where $(a,b)=1$.

A result that waited for **Dirichlet** (18-185) to prove, who could develop new techniques that he called " *of continuous magnitudes*" , that we name today *analytic methods*[47] and proved the celebrated theorem :

Dirichlet (1837) :

there are infinity of prime numbers in every progression $ak+b$ iff $(a,b)=1$

The difficult proof of **Dirichlet** founded a new branch, developed later more by his student Bernhard **Riemann** (1826-1966), which we now name the analytic theory of numbers. It is interesting to read what **Weil** has said about it:

---

[47] In fact , **Euler** has already used analysis in expoloring the number of partitions of an integer n.

*"…In a sense it was born with **Riemann**, who was definitely not a number theorist; it was carried on, among other, by **Hadamard** and later, by **Hardy** who were also not number theorists (I knew **Hadamard** well), and to the best of my understanding, analytic number theory is not number-theory."*

In the same current of ideas, mathematicians see the **Riemann** hypothesis as a problem in complex function theory and not of number theory. But, as the results of this theory are linked to number theory by a way or by another, and as it uses analysis to explore the proprieties of numbers[48], mathematicians have been naming it by this name since long.

In his paper, **Dirichlet** stated that his proof was not completely arithmetic and mentioned that the attempt of **Legendre** to prove it was only by induction. He gave a meaning to the **Euler** product by introducing the real variable x[49]

$$\sum_{n\geq 1}\frac{1}{n^x}=\prod_{p\geq 2}(1-\frac{1}{p^x})^{-1}$$

Euler found that

$$\sum_{n\geq 1}\frac{1}{n^2}=\prod_{p\geq 2}(1-\frac{1}{p^2})^{-1}=\frac{\pi^2}{6}$$

That means again, that there are infinitely many primes. But the primes of the form $p_n = ak + b$, The *period* is a, and b is the first term. which we also note

$$p_n \equiv \ b \ mod(k)$$

For the sequence $10k + 3$ we have the primes p are

---

[48] As algebraic number theory uses algebra, and elementary number theory uses arithmetic and classical algebra.

[49] In fact , he chose the letter s in place of x.

$$3, 13, 23, 43, 53, 73,83,$$

Reminder

in his paper of 1837 , **Dirichlet** did prove that there are infinitely primes in the sequence $a + kb$ only when $k = prime$, the general proof for all $k = any\ integer$ was given in 18 by and **Dedekind**.

dirichlet idea is to that as $\sum_{n\geq 2}\frac{1}{p} = +\infty$ in the same manner he should find a way to prove that

$$\sum_{p=ka+b}\frac{1}{p} = +\infty$$

so to characterize those $p = ka + b$ he introduced a function a *character modulo a* to. **Dirichlet** began his proof for when a is a prime $a = p > 2$

$$n \equiv \zeta^{\gamma}\ (mod\ p)$$

where ζ is primitive root modulo p(see *Elementary Part*), the number γ is called the ***Gauss** index*, that is

$$\zeta^{\gamma} = n$$

and using

$$\zeta^{p-1} = 1$$

Primes are classified by a new function introduced *character de **Dirichlet** modulo p* (1831) or simply *character* noted χ

$$\sum_{n \geq 1} \frac{\chi()}{n^2}$$

When n is not $a + kb$ it is elemintad by the value of the character with period n $\chi(n) = 0$,

For any integer a there are $\varphi(a)$ relatively primes with a,

On a following proprieties of χ

Definition

- $\chi(n) = 0$ if $(a, k) > 1$
- $\chi(n + k) = \chi(n)$
- $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$ (χ is multiplicative)

n $\chi(n) = 0$, thus

$$\sum_{n \geq 1} \frac{\chi(n)}{n^x} = 1 + 0 - 1 + 1 - 1 + 1 + 1 + 0 + \cdots$$

On a pour $k = 9$ on a la fonction les valeurs de $\chi(n)$ modulo 9

n	1	2	3	4	5
$\chi(n)$	1	2	4	5	7

We say that the character $\chi(n)$ modulo m is principal if

$$\chi(n) = \begin{cases} 1 \; if \; (n, m) = 1 \\ 0 \quad otherwise \end{cases}$$

Gives the letter L (thus the famous L –functions):

$$L(x,) = \sum_{n\geq 1} \frac{\chi^{\gamma}}{n^{x}} = \prod_{p\geq 2} (1 - \frac{\chi^{\gamma}}{p^{x}})^{-1}$$

And

$$L_0, \qquad L_1, \qquad L_2, \ldots$$

To characterize the numbers but he only one the reason is a prime numbers so he two primes numbers

p:

q :

Thus has only a finite number of values. on a vu que les residus $mod\ k$ constitue an abelian group,

Théorèm

let $ak + b$ with $(a, b) = 1$, les résidus modulo k constitue an abalien group

This group is prisecily $\frac{\mathbb{Z}}{k\mathbb{Z}}$, then the map χ is a group homomorphism $\frac{\mathbb{Z}}{k\mathbb{Z}}$ et $\mathbb{C}$

$$\chi : \frac{\mathbb{Z}}{k\mathbb{Z}} \longrightarrow \mathbb{C}$$

We know that the number of primitive roots for a given modulo p is $\varphi(p)$

Dirichlet wrote

$$L(\chi, x) = \sum_{n\geq 1} \frac{\chi(ak+b)}{n^x} = \prod_p (1 - \frac{\chi(p)}{p^x})^{-1}$$

He has to prove the essential result

theorem

$$L(\chi, 1) \neq 0$$

Why he did this? because he will take the logarithm

$$logL(\chi, x) = -\sum_p log(1 - \frac{\chi(p)}{p^x})$$

but

$$log\left(1 - \frac{\chi(p)}{p^x}\right) = -\sum_p \frac{\chi^n(p)}{np^{nx}}$$

which gives

$$logL(\chi, x) = \sum_p \sum_n \frac{\chi^n(p)}{np^{nx}}$$

lemma

$$\sum_{pb \bmod k} \frac{1}{p^x} < +\infty$$

When the character is trivial we find the **Riemann** zeta.

Divisor function:

Nous avons vu la divisor function $d(k)$ in the elementary part, Dirichlet a fait des recherches sur cette fonction et by using analytic methods montra le théorème suivant sur le taux de croissance de $d(k)$.

Theorem of Dirichlet (1849) :

$$\sum_{n\leq x} d(n) = xlogx + (2\gamma - 1)x + O(\sqrt{x})$$

The error is $(2\gamma + 1)x + O(\sqrt{x})$. the estimation has been ameliorated since. Mais le problem de trouver la plus petit error, connu sous le nom de *problem de diviseur de Dirichlet* is still open.

To well understand more the signification des symboles '$\boldsymbol{O}$' et '$\boldsymbol{o}$' introduits auparavant on va sur la distribution des nombres premiers

Ça veut dire que $\sum_{p\leq x}\frac{1}{p}$ tend vers $+\infty$ comme $loglogx$. On sait que Euler a écrit heuristiquement

$$\sum \frac{1}{p} = loglog\infty$$

Euler(*Introductio*).

Preuve :

Soit alors

Quadratic forms

we have seen quadratic forms in the elementary part, a binary

$$ax^2 + byx + cy^2$$

Dirichlet , after the work of **Lagrange** and **Gauss**, developed analytic formula for the *class number formula* of a binary quadratic form of determinant D, this formula has been conjectured by **Jacobi** in 1832.

Theorem of **Dirichlet** (1849) :

$$c = xlogx + (2\gamma - 1)x +$$

Pells equation and pigeonhole technic:

A technic invented by **Dirichlet** in 1834. and used a lot by mathematicians. It says that if we have n holes and $n+1$ pigeons then a hole must contain two pigeons. Mathematically if $[0,1]$ is divided in Q intervals : $\left[0,\frac{1}{Q}\right],\left[\frac{1}{Q},\frac{2}{Q}\right],\dots,[\frac{Q-1}{Q},1]$ one of them contains at least two of the points and the distance between them is less then $\frac{1}{Q}$.

Exercises

1) Let b any odd integer . Show that in $b+2n$ infinitly many primes.

1) explain why the identity $\sum_1^{+\infty}\frac{1}{n} = \prod_{p\geq 2}(1-\frac{1}{p})^{-1}$ has no sens

1) find the value of : $\prod_{p\geq 2}(1+\frac{1}{p^3})^{-1}$

1) from $\sum_1^{+\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$, show that there exist infinitely many primes

1) show that : $\chi(1) = 1$

1) calculate modulo 7:

i) χ_{12}

i) χ_{10}

i) χ_{12}

2) show that   that exist infinitely many primes formes : $-1, -3, -7, -9$

2) calculer $\chi(n)$ modulo 3, 6, 5, 9, 11

2) calculer : χ_{12}

2) calculer $\chi(n)$ modulo 3, 6, 5, 9, 11

3) show that $\sum_{k \leq x} d(n) \sim x log x$

Chapter 3

Distribution of Primes

The aim of all these chapters is not only toexpose results be known to the reader,but is the introduction of methods and with the proofs will teach him how the techincs goes then a proof is often very important .

We have seen before that the distribution des nombres premiers est on a la conjecture de **Gauss** d'autres soit les on

$$\pi(x)\{:p \leq x\}$$

alors

$$\pi(x) \sim \int_{2}^{+\infty} \frac{dt}{logt}$$

Ce est connu sous le nombre de théorème des premiers en 1998 par **Hadamard** and **Lavallée-Poussin**.

Pour le nombre des premiers dans une progression $ak + b$ noté $\pi_{a,b}(x)$, on a le résultat du à **Dirichlet**

Theorem

on note $\pi_{a,b}(x)$ le nombre des premiers dans une progression arithmétique $a + bn$ alors

$$\pi_{a,b}(x) \sim \int_{2}^{x} \frac{dt}{logt}$$

La première preuve $\acute{e}l\acute{e}mentaire$ de ce résultat est due au mathématicien russe H.N. Shapiro (1929-2009) en 1950.

Tchebychev work

En 1848 en la conjecture de Bertrand **Tchebychev** a eu introduit deux new functions, ces fonction moins difficile à manier que la fonction $\pi(x)$

Definition

On définit les fonctions ψ et Θ

$$\psi(x) = \sum_{n \leq x} \Lambda(n)$$

et

$$\Theta(x) = \sum_{p \leq x} logp$$

the idea of **Tchebychev** was to simplfy the nature of in to the inequality

$$a \frac{x}{logx} \leq \pi(x) \leq b \frac{x}{logx}$$

we can instead the inequality

$$ax \leq \psi(x) \leq bx$$

by On peut tirer la relation

$$\psi(x) = \Theta(x) + \Theta(x^{1/2}) + \Theta(x^{1/3}) + \cdots$$

On a aussi on a vu que ces fonction arithmétique de la forme

$$g(n) = \sum_{n\geq 1}^{\infty} f(n)$$

Ce qui un résultat intéressant du à Abel

Abel formula(18)

On définit la $\vartheta(x) = \sum_{p\leq x} logp$ alors

$$\vartheta(x) = \sum_{p\leq x} logp$$

C'est une sorte *d'intégration par partie*

Tchebychev au lieu d'étudier la limite $\frac{logx\pi(x)}{x}$ on étudier la limite $\frac{\psi(x)}{x}$ et $\frac{\Theta(x)}{x}$ on a alors

$$\overline{\imath m}\left(\frac{\psi(x)}{x}\right) = \overline{\imath m}\left(\frac{\Theta(x)}{x}\right) = \overline{\imath m}\left(\frac{logx\pi(x)}{x}\right)$$

and

$$\underline{lim}\left(\frac{\psi(x)}{x}\right) = \underline{lim}\left(\frac{\Theta(x)}{x}\right) = \underline{lim}\left(\frac{logx\pi(x)}{x}\right)$$

Dou le résultat de Tchebychev

Tchebychev (18)

$$\overline{\lim}\left(\frac{\psi(x)}{x}\right) \leq 1 \leq \underline{lim}\left(\frac{\psi(x)}{x}\right)$$

Riemann’s zeta function

After **Dirichlet**, **Riemann** worked on the distribution of primes in his famous article of 1859. **Riemann’s** article est l’un des plus beaux masterpiece mathematics of all time. Il a fait une explosion de la analytic numbre theory. Plus de easy understanding of his article voir my book []pour details andtravaux avant 1974 consulter [][][].
on définit la function de Riemann as an infinite series

$$\zeta\ (z) = \sum_{n\geq 1}^{\infty} \frac{1}{n^z}$$

Titshmarsh p.2 says:

> *" the importance of the in ther thoeyr of numbers lies in the fact that it combines two expressions, one theprime and theo ther"*

Apres une continuation analytic au on a

$$\zeta\ (z) = \sin(2z)\zeta\ (z-1)$$

La function ζ est une fonction de théorie des nombre par excellence on a vu des fonction arithmétique que we have vu in the elementary part

$$\zeta\ (z) = \sum_{n\geq 1}^{\infty} \frac{1}{n^z}$$

$$\zeta\ (z) = \sum_{n\geq 1}^{\infty} \frac{1}{n^z} =$$

$$\zeta\ (z) = \sum_{n\geq 1}^{\infty} \frac{1}{n^z} =$$

$$\zeta\ (z) = \sum_{n\geq 1}^{\infty} \frac{1}{n^z} =$$

$\zeta\ (-n) = -\frac{B_{n+1}}{n+1}$ pour $n \geq 0$

If χ_0 is the pricipal caharcter modulo m then

$$L(z, \chi_0) = \zeta\ (z) \prod_{p|m} (1 - \frac{1}{p^z})$$

Après **Euler** les nombres de **Bernoulli** il donna

$$\zeta(2n) = \frac{1}{2n\,!}$$

U problème est comprendre la de on quelque résultats

Théorèm :

$$\zeta\,(z) \;= O(loglogx)$$

Preuve

Soit alors

Prime numbers theorem:

Après Dirichlet, Riemann 1859 qui a enrichi de plus la théorie analytique des nombres. Plus de détails de son article et les work before 1974 consulter []. on définit l

Théorème(TNP) :

$$\pi(x) \sim \frac{x}{logx} \sim \int_{2}^{x} \frac{dt}{logt}$$

they both proved by

$$\psi(x){\sim}x$$

this result has been proved by s élémentaires méthodes by r **Selberg** et **Erdos** en 1849.
On a étrangement le résultat une relation avec la fonction que nous avons vu dans la partie élémentaire le TNP est équivalent aux suivant

Théorème :

$$1)\sum_{n=1}^{+\infty}\frac{\mu(n)}{n} = 0$$

1) $\sum_{n=1}^{+\infty} \Lambda(n) \sim x$

2) $\frac{\vartheta(n)}{n} \sim 0$

3) $\frac{\psi(n)}{n} = 0$

Le théorème nous permet de donne une approximation du nième nombre premier

$$p_n \sim nlogn$$

The result

$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n} = 0$$

Conjtured by **Euler** and proved by **von Mangoldt** (18) and also by **Landau** (1899) in hsi PhD dissertation.

then to find better estimation you regions without zeros and the best if RH is true is

$$\pi(x = \int_2^x \frac{dt}{logt} + O(x^{\frac{1}{2}+a})$$

Tauberians theorems :

In this domain of anlaytic number theory, there existe des résultat très similaire qui ces du au mathématicien allemand Tauber (1-19) cet est du) Norber Wiener(18-19)

Théorème de Wiener(1932) :

Si lim$\int f = \int f =$ alor on lim$\int f = \int f =$

Exercises

3) soit les nombres primes $p_i = 2n_i + 1$. Quel est la distribution des n_i dans $\mathbb{N}$?

2) montrer que les carrées sont moins dense dans $\mathbb{N}$ que les premiers.

3) montrer que $\pi(x) = o(x)$

2) montrer que $\sum_p \frac{1}{p^\sigma}$ converge pour σ >1

1) Montrer que $\sum \frac{1}{p^2}$ converge

2) montrer que $\sum_n \sum_p \frac{1}{np}$ converge

2) montrer que $\sum_n \frac{1}{np^n}$ converge

1) show that : $x^{\pi(x)} \sim e^x$.

2) montrer que $\sum_{p\leq x} \frac{1}{p} \sim \log(\log(x))$

2) montrer que $\sum_{p,n} \frac{1}{pn}$ converge

1) soit p_k et p_{k+1} deux premiers consécutifs, montrer que les séries $\sum_{k=1}^{\infty} \frac{p_{k+1}}{p_k}$ et $\sum_{k=1}^{\infty} \frac{p_k}{p_{k+1}}$ divergent

Chapter 4

Generating functions

In a letter from phi **Naudé**(1-17), **Euler** was asked to study a problem that is partiotion of intger as an example we the number 10 in difert numbers

10=1+9

10=2+7

10=3+7

10=1+2

Then he the idea of a function

$$()()()$$

And will the coeffiets

$$(1+x)(1+x)()$$

Or

$$1+x+x^2+2x^3+2x^4+$$

Then that evry coeficient is the number of of sum aprtion of the power, **Euler** say that the number 8 is 6

$$8 = 8 \qquad 8 = 5 + 3$$

$$8 = 7 + 1 \qquad 8 = 5 + 2 + 1$$

$$8 = 6 + 2 \qquad 8 = 4 + 3 + 1$$

In genral

$$\sum e^{2i} = 1 + 2x + 3x + 4x + \cdots$$

following [**Kar**] we give examples:

so the problem is to estimate the sum and . In

The circle method

In the problem of waring is the colex anlysis

$$\sum n^{it} = e^{itlogm} \sum e^{itlog(1+\frac{n}{m})}$$

g

Exercises

1)

Chapter 5

Weyl's sum

The subject is used in analytic in estimation of zeta function and .

This subject bgan in 1916 when German matheticina Herman **Weyl** (18-19) quetioned[50] about a problem in probability theory on the mean, let be a distribution[51] g so the

$$\sum e^{2i}$$

so the problem is to estimate the sum and . In number hory ***Waring** problem*
then **hardy** and **littlwood**

In **littlwood** used the sum to prove estmation nalely

---

[50] In his article "on "

[51] Th reder is supposed has swith probity theory and statstics so he will no problem in undrstadg this.

$$\pi(x = \int_{2}^{x} \frac{dt}{logt} + O(xe^{-c\sqrt{logx(\log(logx))}}$$

Vinogradov estimates

In **vngrdove** tarfsmed to a polynomial by the nin and the sum becames

$$\sum n^{it} = e^{itlogm} \sum e^{itlog(1+\frac{n}{m})}$$

and coined the name ***Weyls** sum*, to the polynomial

Exercises

1)

Chapter

Multiplacative theory

Multiplicative thery is recent , a classis of **Davenport** said in his classic book (1967)

> *My principal object in these lectures was to give a connected account of analytic number theory in so far as it relates to problems of a multiplicative character, with particular attention to the distribution of primes in arithmetic progression*

A multiplicative n=p…p to other function like the direclet charecter

Exercises

Chapter 1

The L_χ functions

After **Dirichlet** and **Riemann**, Les travaux sur la fonction zêta a suscité des travaux sur d'autres fonctions. Les mathématiciens ont inventé des séries pour variable réel et surtout complexe dites *série de Dirichlet*, qui sont à la base de la *théorie multiplicative des nombres*. Les mathématiciens ont découvert beaucoup d'interactions avec la théorie algébrique des nombres.

Séries de Dirichlet et fonction L() :

Une *série de Dirichle*t est une série infinie de la form

$$\sum_{n\geq 1}^{\infty} \frac{a_n}{n^z}$$

where $a(n)$ are complex numbers, si $a(n) = 1$ on trouve the function $\zeta(z)$.

If the sum is finite i.e.

$$\sum_{n=1}^{N} \frac{a_n}{n^z}$$

it is called ***Direchlet** polynomial*. Mathématiciens ont de choisir de nouvelles fonctions de ces nombres ce sont famous functions L_χ. Is with a in[]:

> *The general rationale of analytic number theory is to derive statastical information about a sequence* $\{a_n\}$ *from the analytic behavior of an appropriate generating function, such as a power series* $\Sigma a_n z^n$ *or a Direchlet series* $\Sigma a_n n^{-z}$.

C'est notamment le *programme de Langlands* qui à comprendre ces séries elles associée aussi une *généraliséd **Riemann** hypothesis.*

Une série de **Dirichlet** a un plan de convergence tandis qu'une série entière a un disque de convergence.

Théorème :

Chaque série de Dirichlet $\sum_{n\geq 1}^{\infty} \frac{a(n)}{n^z}$ a une abscisse de convergence absolue σ_a

Les séries de Dirichlet sont une novelle qui différente des séries entières et ont été étudiées et on leur propriétés. Pour une série entière on ne distingue pas entre convergence absolu et uniforme.

a) Dedekind zeta:

Let the series

$$\zeta_{\mathbb{K}}(z) = \sum_{\mathfrak{a}}^{\infty} \frac{1}{N(\mathfrak{a})}$$

in his suplements (18). where $\mathfrak{a}$ is the number of prime ideals and N the norm of $\mathfrak{a}$. if the algebraic field $\mathbb{K} = \mathbb{Q}$ then $\zeta_{\mathbb{K}}(z)$ is the Riemann zeta function.

Théorèm :

Every Dirichlet series $\sum_{n\geq 1}^{\infty} \frac{a(n)}{n^z}$ a une abscisse de convergence absolue σ_a

In 1917, Erich **Hecke**(1887-1947) proved tha the **Dedekind** zeta function may be continuated to the the complex plan. Landau could prove the same PNT for prime ideals anmly

$$\pi_{\mathbb{K}}(x) \sim \frac{x}{logx}$$

Hecke also introduce his charcters meore then dicrchlet charcters and the Heck Lfunctions defined

$$(z) = \sum_{\mathfrak{a}}^{\infty} \frac{1}{N)}$$

– Hurwitz zeta:

Soit un nombre réel tel 0<u<1 la série

$$\zeta\ (z, u) = \sum_{n\geq 1}^{\infty} \frac{1}{(n+u)^z}$$

est dite zeta de Hurwitz (1-19) il considéra que les rationnels$u$, on montre que

$$L\ (z, \chi) = \frac{1}{n^z} \sum_{r=1}^{n} \chi(r)\, \zeta\ (z, \frac{r}{n})$$

Auusi une rencontre avec les **Bernoulli** polynomials pour $n \geq 0$

$$\zeta\ (-n, u) = -\frac{B_{n+1}(u)}{n+1}$$

Théorème :

Chaque série de Dirichlet $\sum_{n\geq 1}^{\infty} \frac{a(n)}{n^z}$ a une abscisse de convergence absolue σ_a

) d'Epstein zeta function:

soit 0<u<1 la série

$$\zeta_Q(z) = \sum_{(n,m)\neq(0,0)}^{\infty} \frac{1}{Q(n,m)^z}$$

where $Q(n,m)$ is a definie positive quadratic form

$$an^2 + bnm + cm^2$$

is named *d'Epstein's zeta function*, introduit by German mathematicien Paul **Epstein** (1871-1939) in 1903. The numbers a, b, c, n and m are integers with the discriminant(see quadratic froms in Part I) is $D = b^2 - 4ac < 0$.

Théorème :

Chaque série de Dirichlet $\sum_{n\geq 1}^{\infty} \frac{a(n)}{n^z}$ a une abscisse de convergence absolue σ_a

Avec les fonctions il y a une avec les fonctions elliptique. Une fonction elliptique est de la form

$$y^2 = ax^3 + bx + c$$

Le mot du fait que fonction vient de trouver la longueur d'un arc d'ellipse

Hecke series:

Une *série de Dirichle*t est une série infinie de la forme

$$\sum_{n\geq 1}^{\infty} \frac{a(n)}{n^z}$$

Prime ideal theorem

In 1903 **Landau** proved a theorem similar to the PNT in $\mathbb{Z}(\text{or } \mathbb{Q})$ we have

$$\begin{array}{ccc} \mathbb{Z} & \leftrightarrow & \mathbb{K} \\ p & \leftrightarrow & a \end{array}$$

Then the theorem

Theorem :

Chaque série de Dirichlet $\sum_{n\geq 1}^{\infty} \frac{a(n)}{n^z}$ a une abscisse de convergence absolue σ_a

Exercises

3) soit les nombres $\zeta\ (z, u) = \sum_{n\geq 1}^{\infty} \frac{1}{Q(n,m)^z}$ converges

3) soit les nombres $\zeta_K(z) = \sum_{n\geq 1}^{\infty} \frac{a_m}{n^z}$ converges

3) soit les nombres $\zeta\ (z,u) = \sum_{n\geq 1}^{\infty} \frac{1}{Q(n,m)^{z}}$ converges

3) soit les nombres $\zeta\ (z,u) = \sum_{n\geq 1}^{\infty} \frac{1}{Q(n,m)^{z}}$ converges

Chapter 1

Automorphic forms

This a chapter is a continuation of the chapters on the functions of complex variable and their use in number theory. automorphes forms are des fonctions i de la variable complexe z, elles sont utilisés dans beaucoup de branches des mathématiques, mais ce qui nous intéresse ici est leur utilisation dans la théorie des nombres. Aussi les séries de Fourier sont d'utilisation importante dans ce domaine. On se sert des formes modulaires pour ensuite study additive nombres theory.

Elliptic functions:

Theory of elliptic function, initiated by Euler in 1752 in from to the length of the limnescate studied by Fangano(17-17)

$$l = b\int \frac{1}{\sqrt{1-x^4}}dx$$

Then we first elliptic function they are function of complex variables, discovered by Abel and Jacobi in 1827 as inverses to elliptic integrals

$$\int R(x, \sqrt{P_n(x)} dx$$

These integral have been studied previously y Legendre in his classics des *integral elliptiques*(18).

$$u = \int R(z, \sqrt{P_n(z)} dz$$

We inverse by trigonometric substitutions

$$z = f(u)$$

Since these function are periodic (inherited from trigonometric) we first introduce periodic functions. The introduction them to in number theory was by Jacobi who developed

Periodic functions :

On dit f est *périodique* s'il existe a complex number ω tel que

$$f(z + \omega) = f(z)$$

If f has two périodes ω_1 et ω_2 on dit que f est *doublement périodique*. Les périodes constituent in the complex plan des parallélogrammes or a *latice*. Les fonctions périodiques sont étudiées par Legendre puis par Jacobi c'est Jacobi qui a leur utilisation en number theory by using automorphic functions

$$\sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

Abel puis Riemann. this domain is very intéressing ant quand on utilise le nombre complexe z. Alors on a la définition

Definition

une function f est dite elliptique si
- elle est doublement périodique
- elle est méromorphic (has only poles as singularities)

Example

the celebrated *theta function*

$$f(z) = \sum e^{nt+z}$$

We have

Theorem

soit f une fonction elliptique si f n'a pas de pôles ou des zéros alors elle est constante.

Preuve

Puisque f est alors selle est continue, selon le théorème de Liouville elle est constante. Si elle n'a pas de zeros alors 1/f n'a pas de pole de même ■

Function of Weierstrass $\wp(z)$:

Definition

soit f une fonction elliptique si f des zéros

$$\wp(z) = \frac{1}{z^2} + \sum \left\{ \frac{1}{} - \frac{1}{} \right\}$$

And is

La fonction est lus sue la fonction et qui ne rasedant on a la fonction admet l'équation différentielle

$$(y')^2 = 4y - 60y - 140$$

Fonction de Klein $j(z)$:

Modular forms:

we now a very genral new functions *automorphic forms.* On ava voir de nouvelle infinite series ou n'est pas un entier mai a real number, soit la période ω.

Lun des cas particulier important des formes automorphic est les forms modulaires,befor we must *modular group* :

Modular group

Definition

a modular group is the set of matrices $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ tels que $a, b, c\ et\ d \in \mathbb{Z}$ et $Det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = 1$

On a alors pour deu périodes le following result

Definition

deux paire deux paires de périodes (),()sont équivalentes s'il existe une matrice $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ tels que

$$\begin{pmatrix} a \\ a \end{pmatrix} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{pmatrix} a \\ c \end{pmatrix}$$

Eisenstein series:

Eisenstein series are important case of modular forms, Soit un groupe de,

Definition :

the series

$$\sum_{n\geq} \frac{1}{z^{n}}$$

est dite série d’Eisenstein.

On bien l’inverse des rôle des parameter z et n entre une série de Dirichlet et une série d’Eisenstein (n^{-z} becomes z^{-n}) on va voir de new phénomènas.

Le mathématicien allemand Erich Hecke (1887-1947) a joué un rôle il a hypothèse de Riemann en 1917 pour les extensions de corps finis

Langland’s program:

Is a with conjectures about link between number teory and groups .by caandian(19-) in 196

Lagland’’s Lemma :

the series

We have seen before that elliptic ue function and elliptic equation of the form

$$y^2 = ax^3 + bx^2 + cx + d$$

without multiple roots. The thing is that equation has a structure of group its that an elliptic curve there rational numbers. One of the pillar of this theory is Mordell theorem

Theorem of Mordell

f

Exercises

1) Give the differences that you already know between: elliptic integrals elliptic function and elliptic curves.

4) show that a constant is an elliptic function

2) let a *hodograph* function defined as : $f(x) = \frac{ax+b}{cx+d}$.

Calculate : $f^{-1}(x),\ f\left(\frac{1}{x}\right),\ \frac{1}{f(x)}$. What do you remarks?

1) show if ω is a period then $n\omega$ is also a period

1) show if ω_1 and ω_2 are two periods then $n\omega_1 + k\omega_2$ is also periods

1) for what value does the series $\sum_0^{+\infty} e^{-n^2 t}$ converge

Chapter 5

Additive number Theory

We return now to **Waring** problem, the sourcebook of additive number theory. Consider a sequence of integer numbers A, we search how many de nombre can we form adding elements from the sets A, we interested whne give all the natural numbers

$$A + \cdots + A = \mathbb{N}$$

It is evident that if A is the sequence of premiers numbers $\mathbb{P}$, the case $k = 2$ correspont to the **Goldbach** conjecture.

$$(3,5,7,11,13, \dots) + (3,5,7,11,13, \dots) = 2\mathbb{N}$$

Or perhaps we not but at least from an integer n , which gives the expression "all suficiently integers", in this we have the result of **Vinogradov**

$$\mathbb{P} + \mathbb{P} + \mathbb{P} \sim \mathbb{N}$$

The *addition of sequences* operation is the essence of *additive* number theory, as the Russian mathematician Yuri **Linnik**(1915-1972) said[] p.2

> *" Additive number theory studies the proprieties of this operation of adding sequences ; in particular, it describes numbers obtained as a result of the addition of finite number odd sequences, and studies cases when we obtain all integers* $(i.e. \mathbb{N})$ *or all sufficiently large integers "*

We have some old results:

Lagrange(17): every integer is the sum of 4 squares.
Gauss(1796): every integer is the sum of 3 triangular numbers.
Legendre(1813) : every sufficiently integer is the sum of 5 polygonal numbers of order m+2.
Cauchy(1813) : every integer is the sum of polygonial numbers of order m+2
Vinogradov (19) :every sufficiently odd number is the sum of three primes.
Linnik (1943) : every sufficiently odd number is the sum of 7 cubes.

Classical results

Lagrange theorem

Lagarnge is the first proved theorem in additive theory. Fermat claimed that every integer can be written as the sum of of 4 square numbers

$$\mathbb{S} + \mathbb{S} + \mathbb{S} + \mathbb{S} = \mathbb{N}$$

It suffies[52] to prove that every prime number is the sum of four squares. If a^2 and b^2 are two squares then $p = 0 + 0 + 0 + a^2$ is impossible, than we must have $p = 0 + 0 + b^2 + a^2$, so the is to suppose that the following

$$dp = 0 + 1 + b^2 + a^2$$

with $d = 1$ is false

Cauchy theorem

Fermat claimed that every integer can be written as the sum of of $k + 2$ polygonal numbers

$$\mathbb{G}_1 + \cdots + \mathbb{G}_{k+2} = \mathbb{N}$$

Schnirelmann density

In 1930, the Russian mathematician **Schnirelmann** $(1905 - 1938)$ defined a very clever concept[53]: the density of a sequence of integers. Let A a sequence of positive integers

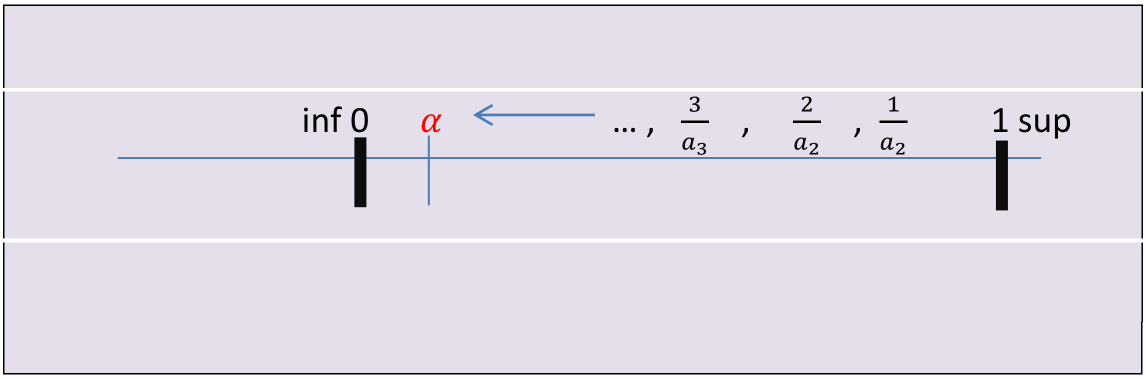
$$0, a_1, a_2, a_3, \dots a_n, \dots$$

He questioned about the limit of the sequence $\frac{n}{a_n}$, and when its limit keeps greater than a positive real number α.

---

[52] Cf. [Nathanson]

[53] Khintchine said: " Schnirelmann first raised the question: to what extent is the density of the sum of several sequences determined solely by the density of the summands, without considering their arithmetical nature". *Three pearls of number theory*.



here a_n is the sequence term of order n. now the definition of the Schnirelmann density:

Definition:

let A (or a_n) a sequence of integers such that

$$A(n) = \sum 1$$

the number of its elements $\leq n$, we define the *density of Schnirelmann* of A linked to the numbers $\frac{A(n)}{n} \geq \alpha$ as:

$$d(A) = \alpha = \inf\left\{\frac{A(n)}{n}\right\}$$

The number 0 is not counted in $A(n)$, we can see that if $1 \notin A$ then $d(A) = 0$, because $d(A) = \frac{0}{1} = 0$.

Example:

The sequence of odd integers: 1,3 ,5 ,7 ,9 , 11, … has for density : $d(A_{odd}) = \frac{1}{2}$ for

$$A_{odd} = \inf\left\{ 1, \quad \frac{2}{3}, \quad \frac{3}{5}, \quad \frac{4}{7}, \dots \right\} = \frac{1}{2}$$

then **Schnirlemann** proved the following lemma :

Lemma: let $C, A\ et\ B$ three sequences of integers , with $C = A + B$, then we have

$$d(C) \geq d(A) + d(B) - d(A)d(B)$$

Suppose that $d(A) = \alpha$, $d(B) = \beta$ and $d(C) = \gamma$ then we want to prove

$$\gamma \geq \alpha + \beta - \alpha\beta$$

All terms of A and B appears in C because $0 \in A$ and B. In C appears also the new terms $a_k + b_k$, so the terms in C are

$$0, \qquad c_k, \qquad a_k\ , \qquad b_k, \qquad a_k + b_k$$

Let $A(n), B(n)$, and $C(n)$ the numbers of terms in each sequence then abviously

$$C(n) > A(n) + B(n)$$

we now look at the terms $a_k + b_k$,they not neither to A not to B . Suppose ther r of them in C then

$$C(n) \geq A(n) \times \sum_{k=1}^{n} r_k$$

This lemma permeated him to prove the following interesting result

Schnirlemann *theorem:*

Let A a sequence of integers such that $0 \in A$, if $d(A) > 0$, then there existe an integer k such that $\forall\, n \in \mathbb{N}$:

$$n = n_1 + \cdots + n_k$$

Otherwise, **Schnirlemann's** theorem says that every sequence A of positive density $(d(A) > 0)$ is a basis for $\mathbb{N}$:

$$A_1 + \cdots + A_k = \mathbb{N}$$

But the inverse is false, there exist sequences A whose density $d(A) = 0$ but are basis for $\mathbb{N}$ as the sequence of squares n^2, theorem of **Lagrange** .

bythis **Schnirelmann** could prove a result about ***Goldbach*** *conjecture*

Schnirlemann(1930) :

$$d(\mathbb{P} + \mathbb{P}) > 0$$

Another theorem more stronger than **Schnirlemann's** would be proved. **Schnirelmann** visited the German number theorist Edmund **Landau** $(1877 - 1938)$ in 1931 at the University of Göttingen, they both conjectured the stronger

$$d(C) \geq d(A) + d(B)$$

A result settled by the American mathematician Henry B. **Mann** (1905-2000).

Mann theorem(1942):

let the sequences : $C = A + B$, then there exists an integer k tels que $\forall$ $n \in \mathbb{N}$:

$$d(C) \geq d(A) + d(B)$$

The proof of this is difficult enough see [**Linnik**]. The theorem eliminates the term $d(A)d(B)$, which it more precise and powerful than **Schnirelmann** theorem if both $d(A)$ and $d(B)$ are > 0.

But since **Mann** has to has proved that he positive density. The problem is that important sequence that interest mathematicians have density 0 like the sequence $\mathbb{P}$, which make the precedent theorems useless. Fortunately Mathematicians haves discovered a new which : essential component

Essential component

Definition

let A a sequence such that and B a sequence of density 0, then B is an essetial component if

$$d(A + B) > d(A)$$

In 19 **Khinchin** discovered that D(a very result

Sieve method :

The method has for origin the known **Eratosthenes** sieve of we have seen in the elementary part chapter 1. More sieve methods plus pousses have been

Developed by **Brun**(18-19) en 19 to prove that the series of prime reciprocal converges .

nrowegian **Selberg** (1-2)

Circle method:

Aditive is by partitions, for example the goldbach conjecture is how is a even integer is partitions.

$$2n = p + p$$

We return as we to the use complex numbers The first to partitions was **Euler** he how many can we write an integer as a sum of different smaller integers, he thus created the *generating series*, see now

Suppose we how many cn write a for example

5=1+4=2+3=

And

$$(1 + x)(1 + x)(1 + x)(1 + x) \dots$$

Euler found if we find the series

$$1 + x + 2x + 3x + 4x + \cdots$$

We he of is 6 and is the coefficient of exponent 8 so a relation between a_n we a series

$$\sum_{n \geq 0} a_n x^n$$

Thi series is called a *generating series* , it genrtes the coefficient a_n or modern genrating function, of course the series is convergent only for the . the seies of Euler weregenrting power series

i) $e = \sum \frac{1}{n!} x^n$ is the number of

i) $tan = \sum \ a_n x$

i) $\sec(x) = \sum \ a_n x$

i) $\sum \ a_n x$

i) $\sum \ a_n x$

Stupendously this idea will be in a a lot of seriesin number theory

i) $\sum \ a_n x$ is the number of

i) $\sum \ a_n x$

i) $\sum \ a_n x$

i) $\sum \ a_n x$

i) $\sum \ a_n x$

a lot of results have been from the method littlewood in it is to

Exercises

1) Why did **Schnirelmann** in his definition of the density d , choose the inf and not the sup?

1) make a comparaison between $a_{k+1} - a_k$ and $\inf\left\{\frac{A(n)}{n}\right\}$

1) why 0 must $\in A$?

1) find the Inf for the following sets

i) $\{2\} \cup]2{,}3[$

ii) $\{1\} \cup [2{,}3[$

iii) $\{2, -1, 0.5\}$

1) let d the **Schnirelmann** density, find $d(A)$ where A is :2, 3,4,5,6,7,8,..the set of natural integers except 1.

1) let A be the sequence : $A = 1{,}4\ {,}5\ {,}8\ {,}9\ {,}\ 12{,}13{,}17, \dots$

i) find $A(n)$ for $n = 1, ,4{,}12, 17.$

ii) let d the **Schnirelmann** density , find the law and calculate : $d(A)$

1) let d the **Schnirelmann** density , calculate : $d(A_{even})$

1) show that : $d(A_{even} + A_{odd}) = 1$. Is $d(A_{odd}) + d(A_{even}) = 1$?

1) prove that the **Schnilermann** density for sequences of squares and cubes is 0.

1) Let a and b be natural integer numbers. Do the following sequences give all natural integers:

i) $2a + 2b + 2$

ii) $2a + 2b + 3$

iii) $2a + 3b + 3$

iv) $2a + 3b$

1) Let k_1, k_2 two integers , does the following sequences give all the integers.

i) $k_1 + 2k_2$

ii) $k_1 + 3k_2$

iii) $k_1 + 4k_2$

1) what about : $k_1 + rk_2$ and $sk_1 + rk_2$, where r and s given integers.

1) show that for integers : $a^2 + f^2 = b^2 + c^2 + d^2 + e^2$

Open problems

We have to signal that a lot of results in number theory not yet proved depend on a big problem in Analysis :the **Riemann** hypotheses or the generalized **Riemann** hypotheses.

1) **Dirichlet** divisor problem.
2) **Riemann** hypotheses.
1) the amount of the roots of the classical zeta function on the critical line is : $\frac{T}{2\pi} log(\frac{T}{2\pi}) - \frac{T}{2\pi}$.
8) are the non-trivial roots of zeta function simple ?

3) Dedekind conjecture, on the Dedekind L-functions.

4) Lindelöf hypotheses(1901) (Riemann hypotheses $\Longrightarrow$ Lindelöf hypotheses).

5) Artin conjecture, on the Artin L-functions(Artin hypotheses $\Longrightarrow$ Dedekind hypotheses).

4) the generalized Riemann hypotheses

6) Ramanujan conjecture , which became Ramanujan-Petersson conjecture

7) the Birch-Swinnerton-Dyer conjecture

9) conjectures de Beilinson

10) Hardy-Littlewood conjectures

11) Selberg conjectures

3) correlation conjecture (or Montgomery conjecture).

1) Find an analytic functions $\boldsymbol{F_i}$ and $L(z,\chi)$ functions such that

i) $\sum_{p\in\mathbb{P}}^{\infty}\frac{1}{p^z} = \boldsymbol{F_1}(L(z,\chi))$

ii) $\sum_{p\in\mathbb{P},n\geq 1}^{\infty}\frac{1}{(p-n)^z} = \boldsymbol{F_2}(L(z,\chi))$

iii) $\sum_{2n>p_i\geq n} \sum_{q_j\leq n}\frac{1}{(n-p_i)^z+(n-q_j)^z} = \boldsymbol{F_3}(L(z,\chi))$

Bibliography and proposed texts

Elementary aspects

[1] **Burton**(D.): Elementary Number Theory (McGraw-Hill 2007)
[3] **LeVeque**(W.): Elementary number theory (Dover 1990)
[3] **Linnik**(W.): methods Elementaires (Gautier-Villars 196)
[1] **Baker** (A.): Transcendental Number Theory (CUP 1974)
[5] **Silverman(J.)** : A friendly introduction to number theory (Pearson 2011)
[5] **Vinogradov(J.)** : number theory (P 19)

Algebraic aspects

[2] **Edwards**(H.): Fermat Last theorem, a genetic introduction to algebraic

number theory (Springer 1977)
[2] **Edwards**(H.): Galois Theory (Springer 1993)
[1] **Samuel**(F.): théorie algébrique des nombres (Herman 1971)
[3] **Bashmakuva**: the beginnings and evolution of Algebra (19)
[1] **Browder**(F.)Editor: Mathematical development arising from Hilbert problems (AMS 1977)
[3] **Kleiner**(I.): ring theory (Birkhauser 1998, p.18-35)
[3] **Mutafian**(C.): Le defi algebrique (Vuibert 198)
[3] **Mutafian**(C.): Equations algébriques (Vuibert 198)
[4] **Queysanne()** : L'Algèbre Modèrne (PUF 1981)
[4] **Rebenboim()** : Therteen lectures on Fermat Last Theorem (PUF 1981)

Analytic aspects

[1] **Apostol**(F.): introduction to analytic number theory (Springer 1976)
[1] **Apostol**(F.): modular forms (Springer 1976)
[1] **Blanchard**(F.): theorie analytique des nombres (19)
[2] **Edwards**(H.): Riemann's Zeta Function (Dover 2001)
[2] **Ivic**(A.): The Theory of The Riemann Zeta-Function With Applications (JW 1985)
[9] **Stopple**(H.) : analytic number theory from to Riemann (Dover 2003)

Miscellany books:

[9] **Yandell**(B.H.) : The Honors Class: Hilbert's Problems and their Solvers (Peters 2002)
[H] **Hardy**(G.) , **Wright**(.): Introduction to The Theory of Numbers (China 2009)

[1] **Kline**(M.): Mathematical thought from ancient to modern times (OUP 1990)
[3] **Narkiewic**(H.): the development of prime number theory from Euclid to Hardy and Littlewood (2007)

[3] **Nathanson**(M.): additive number theory   (springer 200)
[5] **Sandifer(E.)** : How Euler Did It (AMS 200)